SUSE Linux Enterprise Server

11 www.novell.com

26. März 2009 | Verwaltungshandbuch

Verwaltungshandbuch

Für alle Inhalte gilt: Copyright © 2006-2009 Novell, Inc.

Rechtliche Hinweise

Dieses Handbuch ist durch geistige Eigentumsrechte von Novell geschützt. Durch Reproduktion, Vervielfältigung oder Verteilung dieses Handbuchs erklären Sie sich ausdrücklich dazu bereit, die Bestimmungen und Bedingungen dieser Lizenz einzuhalten.

Dieses Handbuch darf allein oder als Teil eines gebündelten Pakets in elektronischer und/oder gedruckter Form frei reproduziert, vervielfältigt und verteilt werden, sofern die folgenden Bedingungen erfüllt sind:

Dieser Copyright-Hinweis und die Namen der Autoren und Beitragenden müssen klar und deutlich in allen reproduzierten, vervielfältigten und verteilten Kopien erscheinen. Dieses Handbuch, insbesondere in gedruckter Form, darf nur zu nichtkommerziellen Verwendung reproduziert und/oder verteilt werden. Vor jeder anderen Verwendung eines Handbuchs oder von Teilen davon ist die ausdrückliche Genehmigung von Novell, Inc., einzuholen.

Eine Liste der Novell-Marken finden Sie in der Liste der Marken und Dienstleistungsmarken unter `http://www.novell.com/company/legal/trademarks/tmlist.html`. Linux* ist eine eingetragene Marke von Linus Torvalds. Alle anderen Drittanbieter-Marken sind das Eigentum der jeweiligen Inhaber. Ein Markensymbol (®, ™ usw.) weist auf eine Novell-Marke hin. Ein Sternchen (*) weist auf eine Drittanbieter-Marke hin.

Alle Informationen in diesem Buch wurden mit größter Sorgfalt zusammengestellt. Doch auch dadurch kann hundertprozentige Richtigkeit nicht gewährleistet werden. Weder Novell, Inc., noch die SUSE LINUX GmbH noch die Autoren noch die Übersetzer können für mögliche Fehler und deren Folgen haftbar gemacht werden.

Inhaltsverzeichnis

Allgemeines zu diesem Handbuch **xi**

Teil I Support und übliche Aufgaben **1**

1 YaST-Online-Update **3**

1.1 Manuelles Installieren von Patches mithilfe der Qt-Schnittstelle 4
1.2 Manuelles Installieren von Patches mithilfe der gtk-Schnittstelle 6
1.3 Automatische Online-Updates 8

2 Erfassen der Systeminformationen für den Support **9**

2.1 Überblick über Novell Support Link 9
2.2 Verwenden von Supportconfig 10
2.3 Übertragen von Informationen an Novell 12
2.4 Weiterführende Informationen 15

3 YaST im Textmodus **17**

3.1 Navigation in Modulen 18
3.2 Einschränkung der Tastenkombinationen 20
3.3 YaST-Kommandozeilenoptionen 21

4 Verwalten von Software mit Kommandozeilen-Tools **23**

4.1 Verwenden von zypper 23
4.2 RPM – der Paket-Manager 29

5 Bash-Shell und Bash-Skripte 41

5.1 Was ist "die Shell"? . . . 41
5.2 Schreiben von Shell-Skripten . . . 47
5.3 Umlenken von Kommandoereignissen . . . 49
5.4 Verwenden von Aliasen . . . 50
5.5 Verwenden von Variablen in der Bash-Shell . . . 50
5.6 Gruppieren und Kombinieren von Kommandos . . . 53
5.7 Arbeiten mit häufigen Ablaufkonstrukten . . . 54
5.8 Weiterführende Informationen . . . 55

Teil II System 57

6 32-Bit- und 64-Bit-Anwendungen in einer 64-Bit-Systemumgebung 59

6.1 Laufzeitunterstützung . . . 60
6.2 Software-Entwicklung . . . 61
6.3 Software-Kompilierung auf Doppelarchitektur-Plattformen . . . 61
6.4 Kernel-Spezifikationen . . . 63

7 Booten und Konfigurieren eines Linux-Systems 65

7.1 Der Linux-Bootvorgang . . . 65
7.2 Der init-Vorgang . . . 70
7.3 Systemkonfiguration über /etc/sysconfig . . . 80

8 Der Bootloader GRUB 85

8.1 Booten mit GRUB . . . 86
8.2 Konfigurieren des Bootloaders mit YaST . . . 96
8.3 Deinstallieren des Linux-Bootloaders . . . 102
8.4 Erstellen von Boot-CDs . . . 103
8.5 Der grafische SUSE-Bildschirm . . . 104
8.6 Fehlersuche . . . 105
8.7 Weiterführende Informationen . . . 106

9 Spezielle Systemfunktionen 109

9.1 Informationen zu speziellen Softwarepaketen . . . 109
9.2 Virtuelle Konsolen . . . 117
9.3 Tastaturzuordnung . . . 117
9.4 Sprach- und länderspezifische Einstellungen . . . 118

10 Druckerbetrieb **123**

10.1 Work-Flow des Drucksystems 125
10.2 Methoden und Protokolle zum Anschließen von Druckern 126
10.3 Installation der Software 126
10.4 Netzwerkdrucker 127
10.5 Grafische Bedienoberflächen für das Drucken 130
10.6 Drucken über die Kommandozeile 131
10.7 Spezielle Funktionen in SUSE Linux Enterprise Server 131
10.8 Fehlersuche 134

11 Gerätemanagemet über dynamischen Kernel mithilfe von udev **143**

11.1 Das `/dev`-Verzeichnis 143
11.2 Kernel-uevents und udev 144
11.3 Treiber, Kernel-Module und Geräte 144
11.4 Booten und erstes Einrichten des Geräts 145
11.5 Überwachen des aktiven udev-Daemons 146
11.6 Einflussnahme auf das Gerätemanagemet über dynamischen Kernel mithilfe von udev-Regeln 147
11.7 Permanente Gerätebenennung 155
11.8 Von udev verwendete Dateien 156
11.9 Weiterführende Informationen 157

12 Das X Window-System **159**

12.1 Manuelles Konfigurieren des X Window-Systems 159
12.2 Installation und Konfiguration von Schriften 167
12.3 Weiterführende Informationen 173

13 Zugriff auf Dateisysteme mit FUSE **175**

13.1 Konfigurieren von FUSE 175
13.2 Einhängen einer NTFS-Partition 175
13.3 Einhängen des entfernten Dateisystems mit SSHFS 177
13.4 Einhängen eines ISO-Dateisystems 177
13.5 Erhältliche FUSE-Plug-Ins 178
13.6 Weiterführende Informationen 178

Teil III Mobile Computer **179**

14 Mobile Computernutzung mit Linux **181**

14.1 Notebooks 181
14.2 Mobile Hardware 190

14.3 Mobiltelefone und PDAs . . . 190
14.4 Weiterführende Informationen . . . 191

15 Energieverwaltung 193

15.1 Energiesparfunktionen . . . 193
15.2 ACPI . . . 194
15.3 Ruhezustand für Festplatte . . . 199
15.4 Fehlersuche . . . 201
15.5 Weiterführende Informationen . . . 203

16 Verwenden von Tablet PCs 205

16.1 Installieren der Tablet PC-Pakete . . . 206
16.2 Konfigurieren des Tablet-Geräts . . . 207
16.3 Verwenden der virtuellen Tastatur . . . 208
16.4 Drehen der Ansicht . . . 209
16.5 Verwenden der Bewegungserkennung . . . 210
16.6 Aufzeichnen von Notizen und Skizzen mit dem Pen . . . 213
16.7 Fehlersuche . . . 215
16.8 Weiterführende Informationen . . . 217

Teil IV Services 219

17 Grundlegendes zu Netzwerken 221

17.1 IP-Adressen und Routing . . . 224
17.2 IPv6 – Das Internet der nächsten Generation . . . 228
17.3 Namensauflösung . . . 238
17.4 Konfigurieren von Netzwerkverbindungen mit YaST . . . 240
17.5 NetworkManager . . . 266
17.6 Manuelle Netzwerkkonfiguration . . . 267
17.7 smpppd als Einwählhelfer . . . 283

18 Drahtlose Kommunikation 287

18.1 Wireless LAN . . . 287

19 SLP-Dienste im Netzwerk 299

19.1 Installation . . . 299
19.2 SLP aktivieren . . . 300
19.3 SLP-Frontends in SUSE Linux Enterprise Server . . . 300
19.4 Installation über SLP . . . 301

19.5 Bereitstellen von Diensten über SLP 301
19.6 Weiterführende Informationen 303

20 Zeitsynchronisierung mit NTP 305

20.1 Konfigurieren eines NTP-Client mit YaST 305
20.2 Manuelle Konfiguration von ntp im Netzwerk 309
20.3 Einrichten einer lokalen Referenzuhr 309
20.4 Uhrensynchronisierung mit einer externen Zeitreferenz (ETR) 310

21 Domain Name System (DNS) 313

21.1 DNS-Terminologie 313
21.2 Installation 314
21.3 Konfiguration mit YaST 315
21.4 Starten des Namenservers BIND 326
21.5 Die Konfigurationsdatei /etc/dhcpd.conf 327
21.6 Zonendateien 332
21.7 Dynamische Aktualisierung von Zonendaten 337
21.8 Sichere Transaktionen 337
21.9 DNS-Sicherheit 339
21.10 Weiterführende Informationen 340

22 DHCP 341

22.1 Konfigurieren eines DHCP-Servers mit YaST 342
22.2 DHCP-Softwarepakete 353
22.3 Der DHCP-Server dhcpd 354
22.4 Weiterführende Informationen 358

23 Verwenden von NetworkManager 359

23.1 Anwendungsbeispiele für NetworkManager 359
23.2 Aktivieren von NetworkManager 360
23.3 Konfigurieren von Netzwerkverbindungen 361
23.4 Verwenden des KDE-Widgets NetworkManager 362
23.5 Verwendung des GNOME NetworkManager-Miniprogramms 363
23.6 NetworkManager und VPN 366
23.7 NetworkManager und Sicherheit 367
23.8 Häufig gestellte Fragen 369
23.9 Fehlersuche 371
23.10 Weiterführende Informationen 372

24 Samba **375**

24.1 Terminologie . . . 375
24.2 Starten und Stoppen von Samba . . . 377
24.3 Konfigurieren eines Samba-Servers . . . 377
24.4 Konfigurieren der Clients . . . 385
24.5 Samba als Anmeldeserver . . . 386
24.6 Samba-Server im Netzwerk mit Active Directory . . . 387
24.7 Weiterführende Informationen . . . 389

25 Verteilte Nutzung von Dateisystemen mit NFS **391**

25.1 Installieren der erforderlichen Software . . . 392
25.2 Importieren von Dateisystemen mit YaST . . . 392
25.3 Manuelles Importieren von Dateisystemen . . . 393
25.4 Exportieren von Dateisystemen mit YaST . . . 395
25.5 Manuelles Exportieren von Dateisystemen . . . 401
25.6 NFS mit Kerberos . . . 404
25.7 Weiterführende Informationen . . . 405

26 Dateisynchronisierung **407**

26.1 Verfügbare Software zur Datensynchronisierung . . . 407
26.2 Kriterien für die Auswahl eines Programms . . . 409
26.3 Einführung in CVS . . . 412
26.4 Einführung in rsync . . . 415
26.5 Weiterführende Informationen . . . 417

27 Der HTTP-Server Apache **419**

27.1 Kurzanleitung . . . 419
27.2 Konfigurieren von Apache . . . 421
27.3 Starten und Beenden von Apache . . . 437
27.4 Installieren, Aktivieren und Konfigurieren von Modulen . . . 440
27.5 Aktivieren von CGI-Skripten . . . 448
27.6 Einrichten eines sicheren Webservers mit SSL . . . 452
27.7 Vermeiden von Sicherheitsproblemen . . . 459
27.8 Fehlersuche . . . 461
27.9 Weiterführende Informationen . . . 462

28 Einrichten eines FTP-Servers mit YaST **465**

28.1 Starten des FTP-Servers . . . 466
28.2 Allgemeine FTP-Einstellungen . . . 467
28.3 FTP-Leistungseinstellungen . . . 468
28.4 Authentifizierung . . . 469

28.5 Einstellungen für Experten 469
28.6 Weitere Informationen 470

29 Der Proxyserver Squid **471**

29.1 Einige Tatsachen zu Proxy-Caches 472
29.2 Systemvoraussetzungen 474
29.3 Starten von Squid 476
29.4 Die Konfigurationsdatei /etc/squid/squid.conf 479
29.5 Konfigurieren eines transparenten Proxy 485
29.6 cachemgr.cgi 488
29.7 Erstellung von Cache-Berichten mit Calamaris 490
29.8 Weiterführende Informationen 491

Allgemeines zu diesem Handbuch

Dieses Handbuch ist für professionelle Netzwerk- und Systemadministratoren zum Betrieb von SUSE® Linux Enterprise konzipiert. Daher soll es nur sicherstellen, dass SUSE Linux Enterprise korrekt konfiguriert ist und die erforderlichen Dienste im Netzwerk verfügbar sind, um eine ordnungsgemäße Funktion gemäß der ursprünglichen Installation zu erlauben. Dieses Handbuch behandelt nicht, wie Sie dafür sorgen, dass SUSE Linux Enterprise die geeignete Kompatibilität mit der Anwendungssoftware Ihres Unternehmens bietet oder dass seine Kernfunktionalität diese Anforderungen erfüllt. Das Handbuch setzt voraus, dass eine vollständige Anforderungsüberprüfung durchgeführt und die Installation angefordert wurde bzw. dass eine Testinstallation zum Zwecke einer solchen Überprüfung angefordert wurde.

Diese Handbuch enthält Folgendes:

Verwaltung
: SUSE Linux Enterprise bietet eine breite Palette an Werkzeugen, um verschiedene Aspekte des Systems anzupassen. In diesem Abschnitt werden einige dieser Aspekte erläutert. Mit einer Übersicht über die erhältlichen Gerätetechnologien, Konfigurationen für hohe Verfügbarkeit und fortgeschrittenen Administrationsmöglichkeiten wird dem Administrator das System vorgestellt.

System
: In diesem Abschnitt wird das zugrunde liegende Betriebssystem umfassend erläutert. SUSE Linux Enterprise unterstützt eine Reihe von Hardware-Architekturen, mit denen Sie Ihre eigenen Anwendungen anpassen können, die auf SUSE Linux Enterprise ausgeführt werden sollen. Der Bootloader und die Informationen zum Bootvorgang unterstützen Sie dabei zu verstehen, wie Ihr Linux-System arbeitet und wie sich Ihre eigenen Skripten und Anwendungen integrieren lassen.

Mobile Computernutzung
: Laptops und die Kommunikation zwischen mobilen Geräten wie PDAs oder Mobiltelefonen und SUSE Linux Enterprise benötigen eine gewisse Aufmerksamkeit. Achten Sie auf geringen Energieverbrauch und sorgen Sie für die Integration verschiedener Geräte in einer sich ändernden Netzwerkumgebung. Machen Sie sich auch mit den Hintergrundtechnologien vertraut, die die erforderliche Funktionalität liefern.

Services
: SUSE Linux Enterprise ist als Netzwerkbetriebssystem konzipiert. Es bietet eine breite Palette an Netzwerkdiensten, z. B. DNS, DHCP, Web, Proxy und Authentifizierung, und fügt sich gut in heterogene Umgebungen mit MS Windows-Clients und -Servern ein.

Viele Kapitel in diesem Handbuch enthalten Links zu zusätzlichen Dokumentationsressourcen. Dazu gehört auch weitere Dokumentation, die auf dem System bzw. im Internet verfügbar ist.

Einen Überblick über die Dokumentation, die für Ihr Produkt verfügbar ist, und die neuesten Dokumentationsupdates finden Sie unter `http://www.novell.com/documentation`.

1 Verfügbare Dokumentation

Wir stellen Ihnen unsere Handbücher in verschiedenen Sprachen in den Formaten HTML und PDF zur Verfügung. Die folgenden Handbücher für Benutzer und Administratoren sind für dieses Produkt verfügbar:

Bereitstellungshandbuch (↑*Bereitstellungshandbuch*)
: Zeigt, wie einzelne oder mehrere Systeme installiert und die produktspezifischen Funktionen für eine Bereitstellungsinfrastruktur genutzt werden. Wählen Sie aus verschiedenen Ansätzen. Von der lokalen Installation über einen Netzwerkinstallationsserver bis zu einer Masseninstallation über eine entfernt gesteuerte, hochgradig angepasste und automatisierte Installationsmethode ist alles möglich.

Verwaltungshandbuch (S. 1)
: Er behandelt Systemverwaltungsaufgaben wie Wartung, Überwachung und Anpassung eines neu installierten Systems.

Security Guide (↑*Security Guide*)
: Zudem werden grundlegende Konzepte der Systemsicherheit vorgestellt, die sowohl lokale als auch netzwerkbezogene Aspekte abdecken. Sie erfahren, wie Sie die einem Produkt inhärente Sicherheitssoftware wie Novell AppArmor verwenden können (diese ermöglicht es Ihnen, für jedes Programm einzeln festzulegen, für welche Dateien Lese-, Schreib- und Ausführungsberechtigungen bestehen) oder das Prüfsystem nutzen können, das zuverlässig Daten zu sicherheitsrelevanten Ereignissen sammelt.

Handbuch für Systemanalyse und Tuning (↑*Handbuch für Systemanalyse und Tuning*)
: Ein Administratorhandbuch zur Problemsuche, Fehlerbehebung und Optimierung. Erfahren Sie, wie Sie Ihr System mithilfe von Überwachungswerkzeugen prüfen und optimieren können und wie Sie Ihre Ressourcen effizient verwalten. Es enthält zudem einen Überblick über häufige Probleme und Lösungen sowie weitere Hilfequellen und Dokumentationsressourcen.

Virtualisierung mit Xen (↑*Virtualisierung mit Xen*)
: Enthält eine Einführung in die Virtualisierungstechnologie Ihres Produkts. Es bietet einen Überblick über die zahlreichen Anwendungsmöglichkeiten und Installationstypen für jede von SUSE Linux Enterprise Server unterstützte Plattform sowie eine Kurzbeschreibung des Installationsvorgangs.

Storage Administration Guide
: Enthält Informationen zur Verwaltung von Speichergeräten auf einem SUSE Linux Enterprise Server.

Neben den umfassenden Handbüchern sind auch mehrere Einführungen für einen schnellen Start verfügbar:

Schnelleinführung zur Installation (↑*Schnelleinführung zur Installation*)
: Listet die Systemanforderungen auf und führt Sie schrittweise durch die Installation von SUSE Linux Enterprise Server von DVD oder einem ISO-Abbild.

Linux Audit Quick Start
: Vermittelt einen kurzen Überblick über die Aktivierung und Konfiguration des Prüfsystems und die Ausführung der wichtigsten Aufgaben wie die Einrichtung von Prüfregeln, die Generierung von Berichten und die Analyse der Protokolldateien.

Novell AppArmor Quick Start
: Unterstützt Sie beim Verstehen der Hauptkonzepte von Novell® AppArmor.

HTML-Versionen der meisten SUSE Linux Enterprise Server-Handbücher finden Sie auf dem installierten System im Verzeichnis `/usr/share/doc/manual` bzw. in den Hilfezentren Ihres Desktops. Die neuesten Dokumentationsaktualisierungen finden Sie unter `http://www.novell.com/documentation`, von wo Sie PDF- oder HTML-Versionen der Handbücher für Ihr Produkt herunterladen können.

2 Rückmeldungen

Für Rückmeldungen stehen mehrere Kanäle zur Verfügung:

- Verwenden Sie für das Melden von Fehlern für eine Produktkomponente oder Verbesserungsvorschläge `https://bugzilla.novell.com/`. Wenn Sie Bugzilla noch nicht kennen, empfehlen wir Ihnen das Dokument *Bug Writing FAQs*, das Sie von der Novell Bugzilla-Homepage herunterladen können.

- Wir freuen uns über Ihre Hinweise, Anregungen und Vorschläge zu diesem Handbuch und den anderen Teilen der Dokumentation zu diesem Produkt. Bitte verwenden Sie die Funktion "Benutzerkommentare" unten auf den einzelnen Seiten der Onlinedokumentation, um Ihre Kommentare einzugeben.

3 Konventionen in der Dokumentation

In diesem Handbuch werden folgende typografische Konventionen verwendet:

- `/etc/passwd`: Dateinamen und Verzeichnisnamen

- *`Platzhalter`*: Ersetzen Sie *`Platzhalter`* durch den tatsächlichen Wert.

- `PATH`: die Umgebungsvariable PATH

- `ls`, `--help`: Befehle, Optionen und Parameter

- `Benutzer`: Benutzer oder Gruppen

- Alt, Alt + F1: Eine Taste oder Tastenkombination. Tastennamen werden wie auf der Tastatur in Großbuchstaben dargestellt.

- *Datei*, *Datei* > *Speichern unter*: Menüelemente, Schaltflächen

- ► **amd64 em64t ipf:** Dieser Absatz ist nur für die angegebenen Architekturen von Bedeutung. Die Pfeile kennzeichnen den Anfang und das Ende des Textblocks. ◄

► **ipseries zseries:** Dieser Absatz ist nur für die angegebenen Architekturen von Bedeutung. Die Pfeile kennzeichnen den Anfang und das Ende des Textblocks. ◄

- *Tanzende Pinguine* (Kapitel *Pinguine*, ↑anderes Handbuch): Dies ist eine Referenz auf ein anderes Handbuch.

Teil I. Support und übliche Aufgaben

1 YaST-Online-Update

Novell stellt fortlaufend Sicherheitsupdates für Ihr Softwareprodukt bereit. Standardmäßig wird openSUSE Updater verwendet, um Ihr System auf dem neuesten Stand zu halten. Weitere Informationen zu openSUSE Updater erhalten Sie unter Abschnitt „System auf dem neuesten Stand halten“ (Kapitel 9, *Installieren bzw. Entfernen von Software*, ↑*Bereitstellungshandbuch*). Dieses Kapitel behandelt das alternative Tool für die Aktualisierung von Software-Paketen: YaST Online Update.

Die aktuellen Patches für SUSE® Linux Enterprise Server finden Sie in einem Repository mit Aktualisierungssoftware. Wenn Sie Ihr Produkt während der Installation registriert haben, ist das Aktualisierungs-Repository bereits konfiguriert. Wenn Sie SUSE Linux Enterprise Server nicht registriert haben, können Sie dies erledigen, indem Sie *Software* > *Online-Update-Konfiguration* in YaST ausführen und *Erweitert* > *Register for Support and Get Update Repository* (Für Support registrieren und Aktualisierungs-Repository beziehen) starten. Alternativ können Sie ein Aktualisierungs-Repository manuell von einer verbürgten Quelle hinzufügen. Starten Sie zum Hinzufügen oder Entfernen von Repositorys den Repository-Manager über *Software* > *Software-Repositorys* in YaST. Weitere Informationen zum Repository Manager finden Sie in Abschnitt „Verwalten von Software-Repositorys und -Diensten“ (Kapitel 9, *Installieren bzw. Entfernen von Software*, ↑*Bereitstellungshandbuch*).

ANMERKUNG: Fehler beim Zugriff auf den Aktualisierungskatalog

Wenn Sie keinen Zugriff auf den Aktualisierungskatalog erhalten, liegt das eventuell daran, dass Ihr Abo abgelaufen ist. Normalerweise wird SUSE Linux Enterprise Server mit einem ein- oder dreijährigen Abo ausgeliefert, durch das

Sie Zugriff auf den Aktualisierungskatalog haben. Dieser Zugriff wird verweigert, sobald das Abo beendet ist.

Bei Verweigerung des Zugriffs auf den Aktualisierungskatalog wird eine Warnmeldung angezeigt, die Ihnen empfiehlt, das Novell Customer Center zu besuchen und Ihr Abo zu überprüfen. Das Novell Customer Center steht Ihnen unter `http://www.novell.com/center/` zur Verfügung.

Novell bietet Aktualisierungen mit verschiedenen Relevanzstufen. Updates vom Typ `Sicherheit` beseitigen ernsthafte Sicherheitsgefahren und sollten auf jeden Fall installiert werden. Updates vom Typ `Empfohlen` beheben Probleme, die zu Schäden an Ihrem Computer führen können, während Updates vom Typ `Optional` Probleme ohne Sicherheitsrelevanz beheben oder Verbesserungen bieten.

Um Aktualisierungen und Verbesserungen mit YaST zu installieren, führen Sie *Software* > *Online-Update* in YaST aus. Alle neuen Patches (außer den optionalen), die derzeit für Ihr System verfügbar sind, sind bereits zur Installation markiert. Klicken Sie auf *Übernehmen* oder *Anwenden*, um die Patches automatisch zu installieren. Bestätigen Sie den Abschluss der Installation mit *Beenden*. Ihr System ist nun auf dem neuesten Stand.

TIPP: Deaktivieren von deltarpms

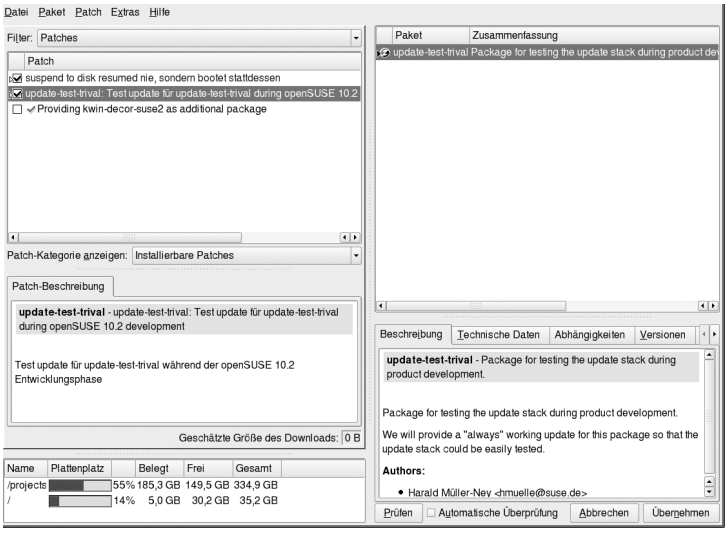
Standardmäßig werden Aktualisierungen als deltarpms heruntergeladen. Da der Neuaufbau von rpm-Paketen aus deltarpms eine Speicher- und CPU-aufwändige Aufgabe ist, können bestimmte Setups oder Hardwarekonfigurationen das Deaktivieren der deltarpms-Verwendung aus Performancegründen erfordern. Um die Verwendung von deltarpms zu deaktivieren, bearbeiten Sie die Datei `/etc/zypp/zypp.conf` und legen `download.use_deltarpm` auf `false` fest.

1.1 Manuelles Installieren von Patches mithilfe der Qt-Schnittstelle

Das Fenster *Online-Update* ist in vier Abschnitte unterteilt. Die Liste aller verfügbaren Patches wird links angezeigt. Unter der Liste der Patches sehen Sie die Beschreibung des ausgewählten Patches. Die rechte Spalte listet die Pakete auf, die im ausgewählten

Patch inbegriffen sind. (Ein Patch kann mehrere Pakete umfassen.) Darunter wird eine ausführliche Beschreibung des ausgewählten Pakets angezeigt. Optional kann die Festplattenauslastung unten in der linken Spalte angezeigt werden (diese Anzeige ist standardmäßig ausgeblendet - verwenden Sie zum Einblenden den gepunkteten Schieber).

Abbildung 1.1 *YaST-Online-Update*


Datei Paket Patch Extras Hilfe
Filter: Patches
Patch
suspend to disk resumed nie, sondern bootet stattdessen
update-test-trival: Test update für update-test-trival during openSUSE 10.2
Providing kwin-decor-suse2 as additional package
Patch-Kategorie anzeigen: Installierbare Patches
Patch-Beschreibung
update-test-trival - update-test-trival: Test update für update-test-trival during openSUSE 10.2 development
Test update für update-test-trival während der openSUSE 10.2 Entwicklungsphase
Geschätzte Größe des Downloads: 0 B
Name Plattenplatz Belegt Frei Gesamt
/projects 55% 185,3 GB 149,5 GB 334,9 GB
/ 14% 5,0 GB 30,2 GB 35,2 GB
Paket Zusammenfassung
update-test-trival Package for testing the update stack during product de
Beschreibung Technische Daten Abhängigkeiten Versionen
update-test-trival - Package for testing the update stack during product development.
Package for testing the update stack during product development.
We will provide a "always" working update for this package so that the update stack could be easily tested.
Authors:
Harald Müller-Nev <hmuelle@suse.de>
Prüfen Automatische Überprüfung Abbrechen Übernehmen

Die Patch-Anzeige listet die für SUSE Linux Enterprise Server verfügbaren Patches auf. Die Patches werden nach Sicherheitsrelevanz sortiert. `security`, `recommended` und `optional`. Patches können in drei verschiedenen Ansichten angezeigt werden. Mit *Patch-Kategorie anzeigen* können Sie die Ansicht wechseln:

Erforderliche Patches (Standardansicht)
: Zurzeit nicht installierte Patches für Pakete, die auf Ihrem System installiert sind.

Nicht erforderliche Patches
: Patches für Pakete, die nicht auf Ihrem System installiert sind, oder Patches , die nicht mehr erforderlich sind (weil bereits von einer anderen Quelle eine Aktualisierung erfolgt ist).

Alle Patches
: Alle für SUSE Linux Enterprise Server verfügbaren Patches.

Ein Listeneintrag besteht aus einem Symbol und dem Patchnamen. Eine Liste der möglichen Symbole erhalten Sie, indem Sie Umschalttaste + F1 drücken. Die erforderlichen Aktionen für Patches der Kategorie `Sicherheit` und `Empfohlen` sind automatisch voreingestellt. Möglich sind die Aktionen *Automatisch installieren*, *Automatisch aktualisieren* oder *Automatisch löschen*. Die Aktionen für `optionale` Patches sind nicht voreingestellt – zur Auswahl einer Aktion klicken Sie mit der rechten Maustaste auf das Patch und wählen Sie die gewünschte Aktion aus.

Wenn Sie ein aktuelles Paket aus einem anderen als dem Aktualisierungs-Repository installieren, können die Anforderungen eines Patches für dieses Paket mit dieser Installation erfüllt sein. In diesem Fall wird ein Häkchen vor der Patchzusammenfassung angezeigt. Das Patch wird in der Liste angezeigt, bis Sie es für die Installation kennzeichnen. Dadurch wird nicht das Patch installiert (da das Paket bereits aktuell ist), sondern das Patch als installiert gekennzeichnet.

Die meisten Patches umfassen Aktualisierungen für mehrere Pakete. Wenn Sie Aktionen für einzelne Pakete ändern möchten, klicken Sie mit der rechten Maustaste auf ein Paket im Paketfenster und wählen Sie eine Aktion. Sobald Sie alle Patches und Pakete wie gewünscht markiert haben, fahren Sie mit *Übernehmen* fort.

1.2 Manuelles Installieren von Patches mithilfe der gtk-Schnittstelle

Das Fenster *Online-Update* ist in zwei Hauptabschnitte unterteilt. Im linken Fensterbereich werden alle Patches aufgelistet sowie verschiedene Filter für die Patch-Liste zur Verfügung gestellt. Im rechten Fensterbereich finden Sie eine Liste der Änderungen, die ausgeführt werden, sobald Sie auf *Anwenden* klicken.

Abbildung 1.2 *YaST-Online-Update*

Filter für die Patch-Liste

Verfügbar
: Zurzeit nicht installierte Patches für Pakete, die auf Ihrem System installiert sind.

Installiert
: Bereits installierte Patches.

Alle
: Bereits installierte oder verfügbare Patches.

Schweregrad
: Zeigen Sie nur die Patches mit der Eigenschaft *Optional*, *Empfohlen* oder *Sicherheit* an. Standardmäßig werden *Alle* Patches angezeigt.

Repositorys
: Mithilfe dieses Filters können Sie die Patches nach Repository anzeigen.

Liste der Pakete
: Wenden Sie hier den benutzerdefinierten Filter an.

Klicken Sie auf einen Patch-Eintrag, um eine Zeile mit detaillierten Informationen zu dem Patch im unteren Bereich des linken Fensterbereichs anzuzeigen. Hier sehen Sie eine detaillierte Beschreibung für den Patch sowie die verfügbaren Versionen. Sie können auf *Installieren* klicken, um optionale Patches zu installieren – Sicherheitspatches und empfohlene Patches sind bereits zur Installation vorausgewählt.

1.3 Automatische Online-Updates

YaST bietet auch die Möglichkeit, eine automatische Aktualisierung einzurichten. Öffnen Sie *Software* > *Online-Update-Konfiguration*. Markieren Sie *Automatisches Online-Update* und wählen Sie *Täglich*, *Wöchentlich* oder *Monatlich* für die Aktualisierungshäufigkeit. Einige Patches, z. B. Kernel-Updates, erfordern Benutzerinteraktion, wodurch der automatische Aktualisierungsprozess angehalten würde. Daher sollten Sie *Interaktive Patches überspringen* aktivieren, wenn der Aktualisierungsvorgang vollautomatisch erfolgen soll. In diesem Fall sollten Sie hin und wieder ein manuelles *Online-Update* ausführen, um Patches zu installieren, bei denen eine Interaktion erforderlich ist.

Erfassen der Systeminformationen für den Support

2

Beim Auftreten eines Problems können Sie mithilfe von `supportconfig` die Systeminformationen erfassen, z. B. die aktuell verwendete Kernel-Version, die Hardware, RPM-Datenbank, Partitionen usw. Das Ergebnis unterstützt das Novell-Supportzentrum dabei, Ihr Problem zu lösen.

2.1 Überblick über Novell Support Link

Novell Support Link (NSL) ist neu bei SUSE Linux Enterprise Server. Es handelt sich dabei um ein Werkzeug, das Systeminformationen sammelt und es Ihnen ermöglicht, diese Informationen für weitere Analysen auf einen anderen Server hochzuladen. Im Novell-Supportzentrum wird Novell Support Link zum Sammeln von Systeminformationen von problematischen Servern verwendet, die anschließend an den öffentlichen FTP-Server von Novell gesendet werden. Die gesammelten Informationen geben Aufschluss über die aktuell verwendete Kernelversion, die Hardware, die RPM-Datenbank, Partitionen etc. Das Ergebnis kann vom Novell-Supportzentrum dazu verwendet werden, Ihre offenen Service-Anforderungen zu lösen.

Sie haben zwei verschiedene Möglichkeiten, Novell Support Link zu verwenden:

1. Verwenden Sie das YaST-Support-Modul oder
2. das Kommandozeilenprogramm `supportconfig`.

Das YaST-Supportmodul ruft zum Sammeln von Informationen `supportconfig` auf.

2.2 Verwenden von Supportconfig

In den folgenden Abschnitten wird die Verwendung von `supportconfig` mit YaST von der Kommandozeile aus einschließlich der möglichen Optionen beschrieben.

2.2.1 Erfassen von Informationen mithilfe von YaST

Gehen Sie wie folgt vor, wenn Sie Ihre Systeminformationen mithilfe von YaST erfassen möchten:

1. Öffnen Sie die URL `http://www.novell.com/center/eservice` und erstellen Sie eine Service-Anforderungsnummer.
2. Starten Sie YaST.
3. Öffnen Sie das *Support*-Modul.
4. Klicken Sie auf *Create report tarball* (Bericht-Tarball erstellen).
5. Wählen Sie eine Option in der Optionsfeldliste aus. Wenn Sie diese zuerst testen möchten, verwenden Sie *Only gather a minimum amount of info* (Nur Mindestmenge an Informationen erfassen). Fahren Sie mit *Weiter* fort.
6. Geben Sie Ihre Kontaktdaten ein. Verwenden Sie Ihre Service-Anforderungsnummer aus Schritt 1 (S. 10) und geben Sie sie in das Textfeld *Novell 11 digit service request number* (11-stellige Novell-Service-Anforderungsnummer) ein. Fahren Sie mit *Weiter* fort.
7. Die Informationserfassung wird gestartet. Fahren Sie nach Ende des Vorgangs mit *Weiter* fort.

8 Prüfen Sie die erfassten Daten und verwenden Sie *Remove from Data* (Aus Daten entfernen), wenn Sie den entsprechenden Dateinamen nicht benötigen. Fahren Sie mit *Weiter* fort.

9 Speichern Sie Ihre Tarball-Datei. Wenn Sie die Daten an das Novell-Kundenzentrum hochladen möchten, stellen Sie sicher, dass *Upload log files tarball into URL* (Protokolldatei-Tarball in URL hochladen) aktiviert ist. Schließen Sie den Vorgang mit *Weiter* ab.

2.2.2 Direkte Verwendung von Supportconfig zum Erfassen der Informationen

Gehen Sie wie folgt vor, wenn Sie `supportconfig` von der Kommandozeile aufrufen möchten:

1 Öffnen Sie eine Shell und melden Sie sich als `root` an.

2 Durch Ausführen von `supportconfig` ohne Auswahl von Optionen werden Standardsysteminformationen gesammelt.

3 Warten Sie, bis das Werkzeug beendet ist.

4 Der Standardspeicherort für das Archiv befindet sich unter `/var/log` und hat das Dateinamenformat `nts_`*`HOST_DATUM_UHRZEIT`*`.tbz`.

2.2.3 Allgemeine Optionen für Supportconfig

Das Dienstprogramm `supportconfig` bietet verschiedene Startoptionen. Die Optionen können mit `supportconfig -h` oder über die man-Seite angezeigt werden. Im Allgemeinen wird `supportconfig` ohne Optionen ausgeführt. Nachfolgend finden Sie eine Zusammenfassung einiger der am meisten verwendeten Startoptionen:

- Verwenden Sie die Minimierungsoption (`-m`), um den Umfang der Informationen, die gesammelt werden, zu minimieren:

  ```
  supportconfig -m
  ```

- In der Ausgabe können Sie weitere Kontaktinformationen hinzufügen (in einer Zeile):

  ```
  supportconfig -E tux@example.org -N "Tux Penguin" -O "Penguin Inc." ...
  ```

- Bei der Fehlersuche zu einem Problem möchten Sie eventuell nur die Informationen zu dem Bereich des Problems sammeln, an dem Sie zurzeit arbeiten. Beispiel: Wenn Sie Probleme mit LVM haben und das betreffende Problem kürzlich bei der Standarausgabe von supportconfig aufgetreten ist. Nachdem Sie die Änderungen durchgeführt haben, sollen die aktuellen LVM-Informationen gesammelt werden. Mit der folgenden Option würden nur die Mindestinformationen zu supportconfig und LVM gesammelt werden.

  ```
  supportconfig -i LVM
  ```

  Zur Anzeige einer vollständigen Liste der Funktionen führen Sie Folgendes aus:

  ```
  supportconfig -F
  ```

- Verwenden Sie die Optionen `-u` und `-r`, um einen supportconfig-Tarball mit der zugehörigen Serviceanforderungsnummer hochzuladen. Beispiel: Angenommen, Sie haben eine Serviceanforderung bei Novell mit der Nachverfolgungsnummer 12345678901 geöffnet, dann führen Sie Folgendes aus:

  ```
  supportconfig -ur 12345678901
  ```

2.3 Übertragen von Informationen an Novell

Sie können das YaST-Supportmodul oder das Kommandozeilendienstprogramm von supportconfig verwenden, um Systeminformationen an Novell zu übertragen. Wenn Sie ein Serverproblem erkannt haben und Unterstützung durch Novell benötigen, müssen Sie eine Serviceanforderung öffnen und die entsprechenden Serverinformationen

an Novell übertragen. Es werden sowohl die YaST-Methoden als auch die Kommandozeilenmethoden beschrieben.

Prozedur 2.1 *Übertragen von Informationen an Novell mithilfe von YaST*

1. Öffnen Sie die URL `http://www.novell.com/center/eservice` und erstellen Sie eine Service-Anforderungsnummer.

2. Schreiben Sie sich die 11-stellige Serviceanforderungsnummer auf. Im folgenden Beispiel wird die Serviceanforderungsnummer 12345678901 angenommen.

3. Klicken Sie im Fenster des YaST-Supportmoduls auf *Berichts-Tarball estellen*.

4. Wählen Sie den Auswahlknopf *Benutzerdefiniert auswählen* aus. Fahren Sie mit *Weiter* fort.

5. Geben Sie Ihre Kontaktinformationen ein, tragen Sie die *11-stellige Serviceanforderungsnummer von Novell* ein und geben Sie die URL für das Uploadziel von Novell an.

   - Verwenden Sie folgende Adresse als sicheres Uploadziel: `https://secure-www.novell.com/upload?appname=supportconfig&file={tarball}`

   - Verwenden Sie folgende Adresse als normales FTP-Uploadziel: `ftp://ftp.novell.com/incoming`

   Fahren Sie fort, indem Sie auf *Weiter* klicken. Es wird nun mit dem Sammeln der Informationen begonnen. Fahren Sie nach Ende des Vorgangs mit *Weiter* fort.

6. Überprüfen Sie die Datensammlung und verwenden Sie *Aus den Daten entfernen*, um alle Dateien zu entfernen, die nicht in dem an Novell hochgeladenen Tarball enthalten sein sollen. Fahren Sie mit *Weiter* fort.

7. Standardmäßig wird eine Kopie des Tarballs unter `/root` gespeichert. Bestätigen Sie, dass Sie eines der oben beschriebenen Uploadziele von Novell verwenden, damit die Option *Protokolldateien-Tarball zu URL hochladen* aktiviert wird. Schließen Sie den Vorgang mit *Weiter* ab.

8. Klicken Sie auf *Fertig stellen*.

Prozedur 2.2 *Weitergeben von Informationen an Novell mithilfe von supportconfig*

1. Öffnen Sie die URL `http://www.novell.com/center/eservice` und erstellen Sie eine Service-Anforderungsnummer.

2. Schreiben Sie sich die 11-stellige Serviceanforderungsnummer auf. Im folgenden Beispiel wird die Serviceanforderungsnummer 12345678901 angenommen.

3. Server mit Internetkonnektivität:

   3a Führen Sie das folgende Kommando aus, um das Standard-Uploadziel zu verwenden:

   ```
   supportconfig -ur 12345678901
   ```

   3b Verwenden Sie als sicheres Uploadziel folgendes Kommando in einer Zeile:

   ```
   supportconfig -r 12345678901 -U
   'https://secure-www.novell.com/upload?appname=supportconfig&file={tarball}'
   ```

4. Server *ohne* Internetkonnektivität

   4a Führen Sie Folgendes aus:

   ```
   supportconfig -r 12345678901
   ```

   4b Laden Sie den Tarball `/var/log/nts_SR12345678901*tbz` manuell an den FTP-Server von Novell (`ftp://ftp.novell.com/incoming`) hoch.

   4c Sie können den Tarball auch an Ihre Serviceanforderung anhängen und die URL für Serviceanforderungen verwenden: `http://www.novell.com/center/eservice`.

5. Sobald sich der Tarball im Verzeichnis `ftp://ftp.novell.com/incoming` befindet, wird er automatisch an Ihre Serviceanforderung angehängt.

2.4 Weiterführende Informationen

Weitere Informationen zum Erfassen von Systeminformationen finden Sie in den folgenden Dokumenten:

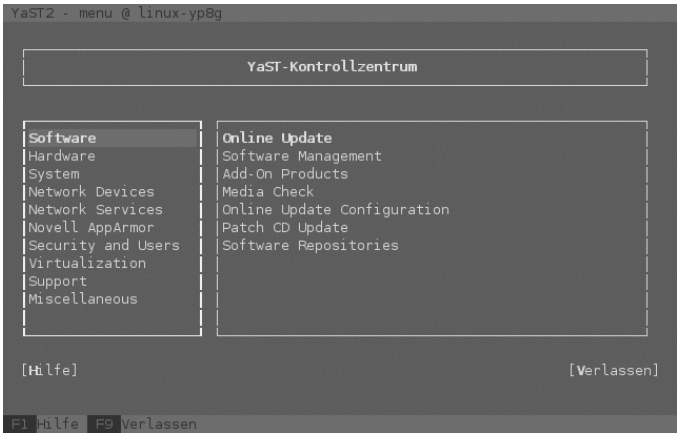
- `man supportconfig` – Die man-Seite von supportconfig
- `man supportconfig.conf` – Die man-Seite der supportconfig-Konfigurationsdatei
- `http://www.novell.com/communities/print/node/4097` – Eine grundlegende Server-Integritätsprüfung mit Supportconfig
- `http://www.novell.com/communities/print/node/4827` – Erstellen Ihres eigenen Supportconfig-Plug-Ins
- `http://www.novell.com/communities/print/node/4800` – Erstellen eines zentralen Supportconfig-Repository

3 YaST im Textmodus

Dieser Abschnitt richtet sich an Systemadministratoren und Experten, die keinen X-Server auf Ihren Systemen ausführen und daher auf das textbasierte Installationswerkzeug angewiesen sind. Der Abschnitt enthält grundlegende Informationen zum Start und Betrieb von YaST im Textmodus.

YaST verwendet im Textmodus die ncurses-Bibliothek, um eine bequeme pseudografische Bedienoberfläche zu bieten. Die ncurses-Bibliothek wird standardmäßig installiert. Die minimale unterstützte Größe des Terminal-Emulators für die Ausführung von YaST beträgt 80 x 25 Zeichen.

Abbildung 3.1 *Hauptfenster von YaST im Textmodus*



Beim Start von YaST im Textmodus wird zuerst das YaST-Kontrollzentrum angezeigt (siehe Abbildung 3.1). Das Hauptfenster besteht aus drei Bereichen. Der linke Bereich, der von einem dicken weißen Rahmen umgeben ist, enthält die Kategorien, zu denen die verschiedenen Module gehören. Die aktive Kategorie wird durch einen farbigen Hintergrund angezeigt. Im rechten Bereich, der von einem dünnen weißen Rahmen umgeben ist, finden Sie eine Übersicht über die in der aktiven Kategorie verfügbaren Module. Der untere Bereich enthält die Schaltflächen für *Hilfe* und *Verlassen*.

Beim Starten des YaST-Kontrollzentrums wird die Kategorie *Software* automatisch ausgewählt. Mit ↓ und ↑ können Sie die Kategorie ändern. Um ein Modul aus der ausgewählten Kategorie zu starten, drücken Sie → Die Modulauswahl ist nun mit einem dicken Rahmen umgeben. Mit ↓ und ↑ können Sie das gewünschte Modul auswählen. Halten Sie die Pfeiltasten gedrückt, um durch die Liste der verfügbaren Module zu blättern. Wenn ein Modul ausgewählt wird, erscheint der Modultitel auf farbigem Hintergrund.

Drücken Sie Eingabetaste, um das gewünschte Modul zu starten. Mehrere Schaltflächen bzw. Auswahlfelder im Modul enthalten einen Buchstaben in einer anderen Farbe (standardmäßig gelb). Mit Alt + gelber_Buchstabe können Sie eine Schaltfläche direkt auswählen und müssen nicht mit Tabulator zu der Schaltfläche wechseln. Verlassen Sie das YaST-Kontrollzentrum durch Drücken von Alt + Q oder durch Auswählen von *Verlassen* und Drücken von Eingabetaste.

3.1 Navigation in Modulen

Bei der folgenden Beschreibung der Steuerelemente in den YaST-Modulen wird davon ausgegangen, dass alle Kombinationen aus Funktionstasten und Alt-Taste funktionieren und nicht anderen globalen Funktionen zugewiesen sind. In Abschnitt 3.2, „Einschränkung der Tastenkombinationen“ (S. 20) finden Sie Informationen zu möglichen Ausnahmen.

Navigation zwischen Schaltflächen und Auswahllisten
: Verwenden Sie Tab, um zwischen den Schaltflächen und Einzelbildern mit den Auswahllisten zu navigieren. Zum Navigieren in umgekehrter Reihenfolge verwenden Sie die Tastenkombinationen Alt + Tab oder Umschalttaste + Tab.

Navigation in Auswahllisten
: Mit den Pfeiltasten (↑ and ↓) können Sie zwischen den einzelnen Elementen in einem aktiven Rahmen, der eine Auswahlliste enthält, navigieren. Wenn einzelne

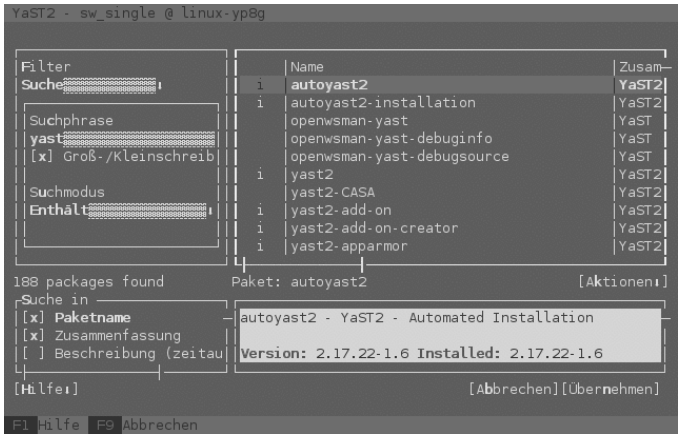
Einträge innerhalb eines Rahmens dessen Breite überschreiten, können Sie mit Umschalttaste + → oder Umschalttaste + ← horizontal nach links bzw. rechts blättern. Alternativ können Sie Strg + E oder Strg + A verwenden. Diese Kombination kann auch verwendet werden, wenn → oder ← zu einem Wechsel des aktiven Rahmens oder der aktuellen Auswahlliste führen würde, wie dies im Kontrollzentrum der Fall ist.

Schaltflächen, Optionsschaltfläche und Kontrollkästchen
: Um Schaltflächen mit leeren eckigen Klammern (Kontrollkästchen) oder leeren runden Klammern (Optionsschaltflächen) auszuwählen, drücken Sie die Leertaste oder Eingabetaste. Alternativ können Optionsschaltflächen und Kontrollkästchen unmittelbar mit Alt + gelber_Buchstabe ausgewählt werden. In diesem Fall brauchen Sie die Auswahl nicht mit Eingabetaste zu bestätigen . Wenn Sie mit Tabulator zu einem Element wechseln, können Sie durch Drücken von Eingabetaste die ausgewählte Aktion ausführen bzw. das betreffende Menüelement aktivieren.

Funktionstasten
: Die F-Tasten (F1 bis F12) bieten schnellen Zugriff auf die verschiedenen Schaltflächen. Verfügbare F-Tastenkürzel werden in der untersten Zeile des YaST-Bildschirms angezeigt. Welche Funktionstasten welchen Schaltflächen zugeordnet sind, hängt vom aktiven YaST-Modul ab, da die verschiedenen Module unterschiedliche Schaltflächen aufweisen ("Details", "Info", "Hinzufügen", "Löschen" usw.). F10 wird für *Übernehmen*, *OK*, *Weiter* und *Beenden* verwendet. Drücken Sie F1, um Zugriff auf die YaST-Hilfe zu erhalten.

Verwenden der Navigationsstruktur im ncurses-Modus
: Einige YaST-Module bieten im linken Fensterbereich eine Navigationsstruktur, in der Konfigurationsdialogfenster ausgewählt werden können. Im ncurses-Modus muss nach der Auswahl in der Navigationsstruktur die Taste Eingabetaste gedrückt werden, um das ausgewählte Dialogfeld anzuzeigen. Dieses beabsichtigte Verhalten erspart zeitraubende Bildaufbauvorgänge beim Blättern durch die Navigationsstruktur.

Abbildung 3.2 *Das Software-Installationsmodul*



3.2 Einschränkung der Tastenkombinationen

Wenn der Fenster-Manager globale Alt-Kombinationen verwendet, funktionieren die Alt-Kombinationen in YaST möglicherweise nicht. Tasten wie Alt oder Umschalttaste können auch durch die Einstellungen des Terminals belegt sein.

Ersetzen von Alt durch Esc
: Tastenkombinationen mit Alt können auch mit Esc anstelle von Alt ausgeführt werden. Esc – H beispielsweise ersetzt Alt + H. (Drücken Sie zunächst Esc, und drücken Sie *dann* H.)

Navigation vor und zurück mit Strg + F und Strg + B
: Wenn die Kombinationen mit Alt und Umschalttaste vom Fenster-Manager oder dem Terminal belegt sind, verwenden Sie stattdessen die Kombinationen Strg + F (vor) und Strg + B (zurück).

Einschränkung der Funktionstasten
: Die F-Tasten werden auch für Funktionen verwendet. Bestimmte Funktionstasten können vom Terminal belegt sein und stehen eventuell für YaST nicht zur Verfügung. Auf einer reinen Textkonsole sollten die Tastenkombinationen mit Alt und die Funktionstasten jedoch stets vollständig zur Verfügung stehen.

3.3 YaST-Kommandozeilenoptionen

Neben der Schnittstelle im Textmodus bietet YaST auch eine reine Kommandozeilenschnittstelle. Eine Liste der YaST-Kommandozeilenoptionen erhalten Sie, wenn Sie Folgendes eingeben:

```
yast -h
```

3.3.1 Starten der einzelnen Module

Um Zeit zu sparen, können die einzelnen YaST-Module direkt gestartet werden. Um ein Modul zu starten, geben Sie Folgendes ein:

```
yast <module_name>
```

Eine Liste aller auf Ihrem System verfügbaren Modulnamen können Sie mit `yast -l` oder `yast --list` anzeigen. Das Netzwerkmodul beispielsweise wird mit `yast lan` gestartet.

3.3.2 Installation von Paketen über die Kommandozeile

Wenn Sie den Namen eines Pakets kennen und das Paket von einer Ihrer aktiven Installations-Repositorys bereitgestellt wird, können Sie das Paket mithilfe der Kommandozeilenoption `-i` installieren.

```
yast -i <Paketname>
```

oder

```
yast --install <Paketname>
```

`Paketname` kann ein einzelner kurzer Paketname sein, beispielsweise `gvim` (solche Pakete werden mit Abhängigkeitsüberprüfung installiert) oder der vollständige Pfad zu einem RPM-Paket, das ohne Abhängigkeitsüberprüfung installiert wird.

Wenn Sie ein kommandozeilenbasiertes Softwareverwaltungs-Dienstprogramm mit Funktionen benötigen, die über die von YaST hinausgehen, sollten Sie möglicherweise zypper verwenden. Dieses neue Dienstprogramm verwendet die Softwareverwaltungs-

bibliothek, die auch die Grundlage des YaST-Paket-Managers bildet. Die grundlegende Verwendung von zypper wird unter Abschnitt 4.1, „Verwenden von zypper“ (S. 23) erläutert.

3.3.3 Kommandozeilenparameter der YaST-Module

Um die Verwendung von YaST-Funktionen in Skripten zu ermöglichen, bietet YaST Kommandozeilenunterstützung für einzelne Module. Die Kommandozeilenunterstützung steht jedoch nicht für alle Module zur Verfügung. Um die verfügbaren Optionen eines Moduls anzuzeigen, geben Sie Folgendes ein:

```
yast <module_name> help
```

Wenn ein Modul keine Kommandozeilenunterstützung bietet, wird es im Textmodus gestartet und es wird folgende Meldung angezeigt.

```
This YaST module does not support the command line interface.
```

Verwalten von Software mit Kommandozeilen-Tools

4

Dieses Kapitel behandelt zypper und RPM, zwei Kommandozeilen-Tools zum Verwalten von Software.

4.1 Verwenden von zypper

zypper ist ein Kommandozeilen-Tool für die Installation und Aktualisierung von Paketen. Die Syntax von zypper ist der Syntax von rug ähnlich. Im Unterschied zu rug benötigt zypper zur Ausführung im Hintergrund den zmd-Daemon nicht. Weitere Informationen über rug-Kompatibilität finden Sie in `man zypper`, Abschnitt "COMPATIBILITY WITH RUG". Damit können Sie Software per Fernzugriff oder mit Hilfe von Shell-Skripten verwalten.

In zypper ist eine Hilfeübersicht integriert:

```
zypper help
```

4.1.1 Allgemeine Verwendung

Die allgemeine Syntax für zypper lautet:

```
zypper [global-options] command [command-options] [arguments] ...
```

Die Komponenten in Klammern sind nicht erforderlich. Am einfachsten führen Sie zypper aus, indem Sie seinen Namen gefolgt von einem Kommando eingeben. Geben Sie z. B. für das Anwenden aller erforderlichen Patches auf den Systemtyp das Folgende ein:

```
zypper patch
```

Zusätzlich können Sie aus einer oder mehreren globalen Optionen wählen, indem Sie sie direkt vor dem Kommando eingeben. Beispielsweise bedeutet `--non-interactive`, dass das Kommando ohne Benutzereingriff ausgeführt wird:

```
zypper --non-interactive patch
```

Um die spezifischen Optionen für ein bestimmtes Kommando zu benutzen, geben Sie sie direkt nach dem Kommando ein. Beispielsweise bedeutet `--auto-agree-with-licenses`, dass alle benötigten Patches auf das System angewendet werden, ohne dass Lizenzen bestätigt werden - alle wurden im Voraus gelesen:

```
zypper patch --auto-agree-with-licenses
```

Einige der Kommandos erfordern ein oder mehrere Argumente:

```
zypper install mplayer
```

Einige der Optionen erfordern ebenfalls ein Argument. Mit nachfolgendem Beispiel werden alle Schemata aufgelistet:

```
zypper search -t pattern
```

Sie können alle obigen Optionen kombinieren. Beispielsweise werden mit Folgendem `mplayer`- und `amarok`-Pakete nur mithilfe des `factory`-Repositorys installiert und ausführlich angegeben:

```
zypper -v install --repo factory mplayer amarok
```

4.1.2 Installieren und Entfernen von Software mit zypper

Um ein Paket aus registrierten Repositorys zu installieren, verwenden Sie:

```
zypper install package_name
```

Verwenden Sie zur Installation eines spezifischen Pakets

```
zypper install package_name=version
```

zypper unterstützt auch Platzhalterzeichen. Wenn Sie bespielsweise alle Pakete installieren möchten, die mit `Paketname` beginnen, geben Sie Folgendes ein:

```
zypper install package_name*
```

Sie können auch ein lokales oder entferntes RPM-Verzeichnis direkt installieren – Zypper installiert auch automatisch alle Pakete, von denen `Paketname` abhängt:

```
zypper install http://www.example.com/package_name.rpm
```

Um ein installiertes Paket zu entfernen, verwenden Sie

```
zypper remove package_name
```

Verwenden Sie zum Installieren und Entfernen von Paketen in einem Vorgang `+/-` oder `~/!` können Sie Pakete auch in einem Schritt installieren und entfernen:

```
zypper install emacs -vim
```

Oder:

```
zypper remove emacs +vim
```

Wenn Sie aber – mit dem zuerst angegebenen Paket verwenden möchten, müssen Sie vor dem Paketnamen `--` eingeben, um die Interpretierung als Kommandooption zu verhindern:

```
zypper install -- -vim emacs
```

WARNUNG: Keine Pakete entfernen, die für das System obligatorisch sind

Entfernen Sie keine Pakete wie `glibc`, `zypper`, `kernel` oder ähnliche. Diese Pakete sind für das System erforderlich, und wenn sie fehlen, ist das System eventuell nicht mehr funktionsfähig.

Standardmäßig verlangt zypper eine Bestätigung, bevor ein ausgewähltes Paket installiert oder entfernt wird oder wenn ein Problem auftritt. Mit der Option `--non-interactive` können Sie diese Bestätigungsabfrage deaktivieren. Die Option muss jedoch vor dem tatsächlich auszuführenden Kommando (Installieren, Entfernen oder Patch) angegeben werden, wie in:

```
zypper --non-interactive install package_name
```

Mit dieser Option kann zypper auch in Skripten und Cron-Aufträgen verwendet werden.

Wenn Sie das entsprechende Quellpaket eines Pakets installieren möchten, verwenden Sie:

```
zypper source-install package_name
```

Mit diesem Kommando installieren Sie auch die Build-Abhängigkeiten des angegebenen Pakets. Wenn Sie dies nicht wünschen, fügen Sie wie folgt den Schalter `--no-build-deps` hinzu:

```
zypper source-install --no-build-deps package_name
```

Natürlich funktioniert dies nur, wenn das Repository mit den Quellpaketen zu Ihrer Repository-Liste hinzugefügt wurde. Geben Sie `zypper search -t srcpackage` ein, um eine Liste der Quellpakete zu erhalten, die in Ihren Repositorys verfügbar sind. Weitere Informationen über das Hinzufügen von Repositorys finden Sie in Abschnitt 4.1.4, „Verwalten von Repositorys“ (S. 27).

Wenn während der Installation ein Fehler auftritt oder Sie die Information aus einem anderen Grund wünschen, prüfen Sie, ob noch alle Abhängigkeiten erfüllt sind:

```
zypper verify
```

4.1.3 Aktualisieren von Software mit zypper

zypper bietet zwei Methoden der Softwareaktualisierung. Wenn Sie alle offiziell verfügbaren Patches in Ihr System integrieren möchten, führen Sie einfach folgendes Kommando aus:

```
zypper patch
```

In diesem Fall werden alle in Ihren Repositorys vorhandenen Patches auf Relevanz überprüft und bei Bedarf installiert. Nach dem Registrieren Ihrer SUSE Linux Enterprise-Installation wird Ihrem System ein offizielles Update-Repository hinzugefügt, das solche Patches enthält. Das obige Kommando ist alles, was Sie brauchen, um sie bei Bedarf anzuwenden.

Wenn ein Repository neue Pakete enthält, aber keine Patches zur Verfügung stellt, zeigt `zypper patch` keinerlei Wirkung. Verwenden Sie zum Aktualisieren aller installierten Pakete mit neueren verfügbaren Versionen:

```
zypper update
```

Verwenden Sie zur Aktualisierung einzelner Pakete das update-Kommando mit den folgenden Argumenten:

```
zypper update package_name
```

Oder das Installationskommando:

```
zypper install package_name
```

Mit dem Kommando kann eine Liste mit allen neu verfügbaren Paketen abgerufen werden:

```
zypper list-updates
```

Verwenden Sie zum Auflisten aller erforderlichen Patches:

```
zypper list-patches
```

4.1.4 Verwalten von Repositorys

Sämtliche Installations- und Patch-Kommandos von zypper sind von der Liste der Repositorys abhängig, die zypper bekannt sind. Um alle dem System bekannten Repositorys aufzulisten, verwenden Sie das Kommando:

```
zypper repos
```

Das Ergebnis ist der folgenden Ausgabe ähnlich:

```
# | Alias                              | Name
   | Enabled | Refresh
--+------------------------------------+-----------------------------------+--------+-------
1 | SUSE-Linux-Enterprise-Server 11-0 | SUSE-Linux-Enterprise-Server 11-0
  | Yes     | No
2 | SLES-11-Updates                    | SLES 11 Online Updates
   | Yes     | Yes
3 | broadcomdrv                        | Broadcom Drivers
   | Yes     | No
```

Bei der Angabe von Repositorys kann in verschiedenen Kommandos ein Alias, URI oder eine Repository-Nummber aus der Ausgabe des Kommandos `zypper repos` verwendet werden. Beachten Sie jedoch, dass sich Nummern nach dem Bearbeiten der Repository-Liste ändern können. Der Alias ändert sich nie von alleine.

Wenn ein Repository von der Liste entfernt werden soll, verwenden Sie das Kommando `zypper removerepo` zusammen mit dem Alias oder der Nummer des zu löschenden Repositorys. Zum Entfernen der `Broadcom Drivers` aus dem Beispiel verwenden Sie das folgende Kommando:

```
zypper removerepo 3
```

Zum Hinzufügen eines Repository, führen Sie Folgendes aus:

```
zypper addrepo URI Alias
```

URI kann ein Internet-Repository, ein Verzeichnis oder eine CD oder DVD sein. Der *Alias* ist ein Kürzel und eine eindeutige Kennung für das Repository. Sie können ihn frei wählen, vorausgesetzt, er ist eindeutig. zypper gibt eine Warnung aus, wenn Sie einen Alias angeben, der bereits verwendet wird.

Um das Arbeiten mit Repositorys bequemer zu gestalten, verwenden Sie kurze und einprägsame Aliasbezeichnungen. Ein Repository-Alias kann mit dem Kommando `renamerepo` geändert werden. Wenn Sie beispielsweise die lange Angabe `SUSE-Linux-Enterprise-Server 11-0` im Beispiel zur knappen Bezeichnung `main` ändern möchten, geben Sie Folgendes ein:

```
zypper renamerepo 1 main
```

4.1.5 Abfragen

Verschiedene Abfragekommandos wie `search`, `info` oder `what-provides` stehen zur Verfügung.

`search` betrifft Paketnamen oder optional Paketzusammenfassungen und -beschreibungen und zeigt Statusinformationen (`S`) in der ersten Spalte der Liste der gefundenen Pakete.

`info` mit einem Paketnamen als Argument zeigt ausführliche Informationen über ein Paket an.

Das `what-provides-`*`Paket`* gleicht dem `rpm -q --whatprovides-`*`Paket`*, aber rpm ist nur für Abfragen der RPM-Datenbank (die Datenbank aller installierten Pakete) möglich. zypper informiert Sie auf der anderen Seite über Anbieter der Möglichkeit von einem beliebigen Repository, nicht nur von denen, die installiert sind.

Weitere Abfragekommandos und ausführliche Nutzungsinformationen finden Sie auf der zypper-man-Seite (`man zypper`).

4.1.6 Weiterführende Informationen

Geben Sie für weitere Informationen zur Verwaltung von Software `zypper help` oder `zypper help` in die Kommandozeile ein oder rufen Sie die man-Seite `zypper(8)` auf.

4.2 RPM – der Paket-Manager

RPM (RPM Package Manager) wird für die Verwaltung von Softwarepaketen verwendet. Seine Hauptbefehle lauten `rpm` und `rpmbuild`. In der leistungsstarken RPM-Datenbank können Benutzer, Systemadministratoren und Paketersteller ausführliche Informationen zur installierten Software abfragen.

Im Wesentlichen hat `rpm` fünf Modi: Installieren, Deinstallieren oder Aktualisieren von Software-Paketen; Neuaufbauen der RPM-Datenbank, Abfragen der RPM-Basis oder individuellen RPM-Archiven, Integritätsprüfung der Pakete und Signieren von Paketen. `rpmbuild` ermöglicht das Aufbauen installierbarer Pakete von Pristine-Quellen.

Installierbare RPM-Archive sind in einem speziellen binären Format gepackt. Diese Archive bestehen aus den zu installierenden Programmdateien und aus verschiedenen Metadaten, die bei der Installation von `rpm` benutzt werden, um das jeweilige Softwarepaket zu konfigurieren, oder die zu Dokumentationszwecken in der RPM-Datenbank gespeichert werden. RPM-Archive haben für gewöhnlich die Dateinamenserweiterung `.rpm`.

TIPP: Pakete zur Software-Entwicklung

Bei etlichen Paketen sind die zur Software-Entwicklung erforderlichen Komponenten (Bibliotheken, Header- und Include-Dateien usw.) in eigene Pakete ausgelagert. Diese Entwicklungspakete werden nur benötigt, wenn Sie Software selbst kompilieren möchten – beispielsweise die neuesten GNOME-Pakete. Solche Pakete sind am Namenszusatz `-devel` zu erkennen, z. B. die Pakete `alsa-devel`, `gimp-devel` und `kdelibs3-devel`.

4.2.1 Prüfen der Authentizität eines Pakets

RPM-Pakete sind mit GnuPG signiert. Der Schlüssel mit dem "Fingerabdruck" lautet:

```
1024D/9C800ACA 2000-10-19 SuSE Package Signing Key <build@suse.de>
Key fingerprint = 79C1 79B2 E1C8 20C1 890F  9994 A84E DAE8 9C80 0ACA
```

Mit dem Befehl `rpm --checksig` *`paket`*`-1.2.3.rpm` können Sie die Signatur eines RPM-Pakets überprüfen und feststellen, ob es wirklich von SUSE oder einer anderen vertrauenswürdigen Quelle stammt. Dies ist insbesondere bei Update-Paketen aus dem Internet zu empfehlen. Der öffentliche Paketsignierschlüssel von SUSE ist standardmäßig in `/root/.gnupg/` hinterlegt. Der Schlüssel befindet sich zusätzlich im Verzeichnis `/usr/lib/rpm/gnupg/`, damit auch normale Benutzer die Signatur von RPM-Paketen prüfen können.

4.2.2 Verwalten von Paketen: Installieren, Aktualisieren und Deinstallieren

In der Regel kann ein RPM-Archiv einfach installiert werden: `rpm -i` *`package`*`.rpm`. Mit diesem Befehl wird das Paket aber nur dann installiert, wenn seine Abhängigkeiten erfüllt sind und keine Konflikte mit anderen Paketen bestehen. rpm `fordert per Fehlermeldung die Pakete an, die zum Erfüllen der Abhängigkeiten installiert werden müssen.` Im Hintergrund stellt die RPM-Datenbank sicher, dass keine Konflikte entstehen: Jede spezifische Datei darf nur zu einem Paket gehören. Durch die Wahl anderer Optionen können Sie `rpm` zwingen, diese Standards zu ignorieren, jedoch ist dies nur für Spezialisten gedacht. Andernfalls wird damit die Integrität des Systems gefährdet und möglicherweise die Update-Fähigkeit aufs Spiel gesetzt.

Die Optionen `-U` oder `--upgrade` und `-F` oder `--freshen` können für das Update eines Pakets benutzt werden, z. B.: `rpm -F` *`paket`*`.rpm`. Dieser Befehl entfernt die Dateien der alten Version und installiert sofort die neuen Dateien. Der Unterschied zwischen den beiden Versionen besteht darin, dass mit `-U` auch Pakete installiert werden, die vorher nicht im System vorhanden waren, wohingegen mit `-F` nur zuvor installierte Pakete aktualisiert werden. Bei einem Update verwendet `rpm` zur sorgfältigen Aktualisierung der Konfigurationsdateien die folgende Strategie:

- Falls eine Konfigurationsdatei vom Systemadministrator nicht geändert wurde, installiert `rpm` die neue Version der entsprechenden Datei. Es sind keine Eingriffe seitens des Administrators nötig.

- Falls eine Konfigurationsdatei vom Systemadministrator vor dem Update geändert wurde, speichert `rpm` die geänderte Datei mit der Erweiterung `.rpmorig` oder `.rpmsave` (Sicherungsdatei) und installiert nur dann die Version aus dem neuen Paket, wenn sich die ursprünglich installierte Datei und die neue Version unterscheiden. Vergleichen Sie in diesem Fall die Sicherungsdatei (`.rpmorig` oder `.rpmsave`) mit der neu installierten Datei und nehmen Sie Ihre Änderungen erneut in der neuen Datei vor. Löschen Sie anschließend unbedingt alle `.rpmorig`- und `.rpmsave`-Dateien, um Probleme mit zukünftigen Updates zu vermeiden.

- `.rpmnew`-Dateien erscheinen immer dann, wenn die Konfigurationsdatei bereits existiert *und* wenn die Kennung `noreplace` mit der `.spec`-Datei angegeben wurde.

Im Anschluss an ein Update sollten alle `.rpmsave`- und `.rpmnew`-Dateien nach einem Abgleich entfernt werden, damit sie bei zukünftigen Updates nicht stören. Die Erweiterung `.rpmorig` wird zugewiesen, wenn die Datei zuvor nicht von der RPM-Datenbank erkannt wurde.

Andernfalls wird `.rpmsave` verwendet. Mit anderen Worten: `.rpmorig` entsteht bei einem Update von einem Fremdformat auf RPM. `.rpmsave` entsteht bei einem Update aus einem älteren RPM auf einen neueren RPM. `.rpmnew` informiert nicht darüber, ob der Systemadministrator die Konfigurationsdatei geändert hat. Eine Liste all dieser Dateien ist in `/var/adm/rpmconfigcheck` verfügbar. Einige Konfigurationsdateien (wie `/etc/httpd/httpd.conf`) werden nicht überschrieben, um den weiteren Betrieb zu ermöglichen.

Der Schalter `-U` ist *nicht* einfach gleichbedeutend mit der Deinstallation mit der Option `-e` und der Installation mit der Option `-i`. Verwenden Sie `-U`, wann immer möglich.

Geben Sie `rpm -e` *`paket`* ein, wenn Sie ein Paket entfernen möchten. `rpm` löscht das Paket nur, wenn keine nicht erfüllten Abhängigkeiten vorhanden sind. Theoretisch ist es unmöglich, beispielsweise Tcl/Tk zu löschen, solange eine andere Anwendung Tcl/Tk noch benötigt. Auch in diesem Fall nutzt RPM die Datenbank zur Unterstützung. Falls es in Ausnahmefällen nicht möglich ist, zu löschen, obwohl *keine* zusätzlichen

Abhängigkeiten bestehen, können Sie versuchen, die RPM-Datenbank mit der Option `--rebuilddb` neu aufzubauen.

4.2.3 RPM und Patches

Um die Betriebssicherheit eines Systems zu garantieren, müssen von Zeit zu Zeit Update-Pakete auf dem System installiert werden. Bisher konnte ein Fehler in einem Paket nur eliminiert werden, indem das vollständige Paket ersetzt wurde. Bei großen Paketen mit Fehlern in kleinen Dateien kann dies schnell zu großen Datenmengen führen. Jedoch bietet SUSE RPM nun eine Funktion, mit der Patches in Pakete installiert werden können.

Die wichtigsten Überlegungen dazu werden am Beispiel "pine" aufgezeigt:

Ist der Patch-RPM für mein System geeignet?
: Um dies zu prüfen, fragen Sie zunächst die installierte Version des Pakets ab. Im Fall von pine verwenden Sie den Befehl:

```
rpm -q pine
pine-4.44-188
```

Prüfen Sie dann, ob der Patch-RPM sich für diese Version von pine eignet:

```
rpm -qp --basedon pine-4.44-224.i586.patch.rpm
pine = 4.44-188
pine = 4.44-195
pine = 4.44-207
```

Dieser Patch passt zu drei verschiedenen Versionen von pine. Auch die im Beispiel installierte Version wird aufgeführt, d. h. der Patch kann installiert werden.

Welche Dateien werden durch den Patch ersetzt?
: Die durch einen Patch betroffenen Dateien können leicht im Patch-RPM abgelesen werden. Der `rpm`-Parameter `-P` ermöglicht die Auswahl von speziellen Patch-Funktionen. Zeigen Sie die Dateiliste mit dem folgenden Befehl an:

```
rpm -qpPl pine-4.44-224.i586.patch.rpm
/etc/pine.conf
/etc/pine.conf.fixed
/usr/bin/pine
```

Oder verwenden Sie, falls der Patch bereits installiert ist, den folgenden Befehl:

```
rpm -qPl pine
/etc/pine.conf
/etc/pine.conf.fixed
/usr/bin/pine
```

Wie kann ein Patch-RPM im System installiert werden?

Patch-RPMs werden wie normale RPMs verwendet. Der einzige Unterschied liegt darin, dass ein passender RPM bereits installiert sein muss.

Welche Patches sind bereits auf dem System installiert und zu welchen Paketversionen gehören sie?

Eine Liste aller im System installierter Patches kann über den Befehl `rpm -qPa` angezeigt werden. Wenn nur ein Patch in einem neuen System installiert ist (wie in unserem Beispiel), sieht die Liste wie folgt aus:

```
rpm -qPa
pine-4.44-224
```

Wenn Sie zu einem späteren Zeitpunkt wissen möchten, welche Paketversion ursprünglich installiert war, können Sie auch diese Information der RPM-Datenbank entnehmen. Für `pine` rufen Sie diese Information mit dem folgenden Befehl ab:

```
rpm -q --basedon pine
pine = 4.44-188
```

Weitere Informationen, auch zur Patch-Funktion von RPM, stehen auf den man-Seiten von `rpm` und `rpmbuild` zur Verfügung.

4.2.4 Delta-RPM-Pakete

Delta-RPM-Pakete enthalten die Unterschiede zwischen einer alten und einer neuen Version eines RPM-Pakets. Wenn Sie ein Delta-RPM auf ein altes RPM anwenden, ergibt dies einen vollständig neuen RPM. Es ist nicht erforderlich, dass eine Kopie des alten RPM vorhanden ist, da ein Delta-RPM auch mit einem installierten RPM arbeiten kann. Die Delta-RPM-Pakete sind sogar kleiner als Patch-RPMs, was beim Übertragen von Update-Paketen über das Internet von Vorteil ist. Der Nachteil ist, dass Update-Vorgänge mit Delta-RPMs erheblich mehr CPU-Zyklen beanspruchen als normale oder Patch-RPMs.

Die Binärdateien `prepdeltarpm`, `writedeltarpm` und `applydeltarpm` sind Teil der Delta-RPM-Suite (Paket `deltarpm`) und helfen Ihnen beim Erstellen und Anwenden von Delta-RPM-Paketen. Mit den folgenden Befehlen erstellen Sie ein

Delta-RPM mit dem Namen `new.delta.rpm`. Der folgende Befehl setzt voraus, dass `old.rpm` und `new.rpm` vorhanden sind:

```
prepdeltarpm -s seq -i info old.rpm > old.cpio
prepdeltarpm -f new.rpm > new.cpio
xdelta delta -0 old.cpio new.cpio delta
writedeltarpm new.rpm delta info new.delta.rpm
```

Entfernen Sie zum Schluss die temporären Arbeitsdateien `old.cpio`, `new.cpio` und `delta`.

Mit `applydeltarpm` können Sie den neuen RPM aus dem Dateisystem rekonstruieren, wenn das alte Paket bereits installiert ist:

```
applydeltarpm new.delta.rpm new.rpm
```

Um es aus dem alten RPM abzuleiten, ohne auf das Dateisystem zuzugreifen, verwenden Sie die Option `-r`:

```
applydeltarpm -r old.rpm new.delta.rpm new.rpm
```

Technische Details finden Sie in `/usr/share/doc/packages/deltarpm/README`.

4.2.5 RPM Abfragen

Mit der Option `-q` initiiert `rpm` Abfragen und ermöglicht es, ein RPM-Archiv zu prüfen (durch Hinzufügen der Option `-p`) und auch die RPM-Datenbank nach installierten Paketen abzufragen. Zur Angabe der benötigten Informationsart stehen mehrere Schalter zur Verfügung. Weitere Informationen hierzu finden Sie unter Tabelle 4.1, „Die wichtigsten RPM-Abfrageoptionen“ (S. 34).

Tabelle 4.1 *Die wichtigsten RPM-Abfrageoptionen*

`-i`	Paketinformation
`-l`	Dateiliste
`-f FILE`	Abfrage nach Paket, das die Datei *`FILE`* enthält. (*`FILE`* muss mit dem vollständigen Pfad angegeben werden.)

`-s`	Dateiliste mit Statusinformation (impliziert `-l`)
`-d`	Nur Dokumentationsdateien auflisten (impliziert `-l`)
`-c`	Nur Konfigurationsdateien auflisten (impliziert `-l`)
`--dump`	Dateiliste mit vollständigen Details (mit `-l`, `-c` oder `-d` benutzen)
`--provides`	Funktionen des Pakets auflisten, die ein anderes Paket mit `--requires` anfordern kann
`--requires`, `-R`	Fähigkeiten, die das Paket benötigt
`--scripts`	Installationsskripten (preinstall, postinstall, uninstall)

Beispielsweise gibt der Befehl `rpm -q -i wget` die in Beispiel 4.1, „rpm -q -i wget“ (S. 35) gezeigte Information aus.

Beispiel 4.1 *rpm -q -i wget*

```
Name        : wget                         Relocations: (not relocatable)
Version     : 1.9.1                             Vendor: SUSE LINUX AG,
Nuernberg, Germany
Release     : 50                            Build Date: Sat 02 Oct 2004
03:49:13 AM CEST
Install date: Mon 11 Oct 2004 10:24:56 AM CEST      Build Host: f53.suse.de
Group       : Productivity/Networking/Web/Utilities   Source RPM:
wget-1.9.1-50.src.rpm
Size        : 1637514                          License: GPL
Signature   : DSA/SHA1, Sat 02 Oct 2004 03:59:56 AM CEST, Key ID
a84edae89c800aca
Packager    : http://www.suse.de/feedback
URL         : http://wget.sunsite.dk/
Summary     : A tool for mirroring FTP and HTTP servers
Description :
Wget enables you to retrieve WWW documents or FTP files from a server.
This can be done in script files or via the command line.
[...]
```

Die Option `-f` funktioniert nur, wenn Sie den kompletten Dateinamen mit dem vollständigen Pfad angeben. Sie können so viele Dateinamen wie nötig angeben. Beispielsweise führt der folgende Befehl

```
rpm -q -f /bin/rpm /usr/bin/wget
```

zum Ergebnis:

```
rpm-4.1.1-191
wget-1.9.1-50
```

Wenn nur ein Teil des Dateinamens bekannt ist, verwenden Sie ein Shell-Skript, wie in Beispiel 4.2, „Skript für die Suche nach Paketen“ (S. 36) gezeigt. Übergeben Sie den partiellen Dateinamen als Parameter beim Aufruf des Skripts.

Beispiel 4.2 *Skript für die Suche nach Paketen*

```
#! /bin/sh
for i in $(rpm -q -a -l | grep  $1); do
    echo "\"$i\" is in package:"
    rpm -q -f $i
    echo ""
done
```

Der Befehl `rpm -q --changelog rpm` zeigt eine detaillierte Liste der Änderungsinformation zu einem bestimmten Paket nach Datum sortiert. Dieses Beispiel zeigt Informationen zum Paket `rpm`.

Mithilfe der installierten RPM-Datenbank sind Überprüfungen möglich. Initiieren Sie die Überprüfungen mit `-V`, `-y` oder `--verify`. Mit dieser Option zeigt `rpm` alle Dateien in einem Paket an, die seit der Installation geändert wurden. `rpm` verwendet acht verschiedene Zeichen als Hinweis auf die folgenden Änderungen:

Tabelle 4.2 *RPM-Überprüfungsoptionen*

`5`	MD5-Prüfsumme
`S`	Dateigröße
`L`	Symbolischer Link
`T`	Änderungszeit
`D`	Major- und Minor-Gerätenummern
`U`	Eigentümer

G	Gruppe
M	Modus (Berechtigungen und Dateityp)

Bei Konfigurationsdateien wird der Buchstabe `c` ausgegeben. Beispielsweise für Änderungen an `/etc/wgetrc` (`wget`):

```
rpm -V wget
S.5....T c /etc/wgetrc
```

Die Dateien der RPM-Datenbank werden in `/var/lib/rpm` abgelegt. Wenn die Partition `/usr` eine Größe von 1 GB aufweist, kann diese Datenbank beinahe 30 MB belegen, insbesondere nach einem kompletten Update. Wenn die Datenbank viel größer ist als erwartet, kann es nützlich sein, die Datenbank mit der Option `--rebuilddb` neu zu erstellen. Legen Sie zuvor eine Sicherungskopie der alten Datenbank an. Das `cron`-Skript `cron.daily` legt täglich (mit gzip gepackte) Kopien der Datenbank an und speichert diese unter `/var/adm/backup/rpmdb`. Die Anzahl der Kopien wird durch die Variable `MAX_RPMDB_BACKUPS` (Standard: `5`) in `/etc/sysconfig/backup` gesteuert. Die Größe einer einzelnen Sicherungskopie beträgt ungefähr 1 MB für 1 GB in `/usr`.

4.2.6 Installieren und Kompilieren von Quellpaketen

Alle Quellpakete haben die Erweiterung `.src.rpm` (Source-RPM).

TIPP

Quellpakete können vom Installationsmedium auf die Festplatte kopiert und mit YaST entpackt werden. Sie werden im Paket-Manager jedoch nicht als installiert (`[i]`) gekennzeichnet. Das liegt daran, dass die Quellpakete nicht in der RPM-Datenbank eingetragen sind. Nur *installierte* Betriebssystemsoftware wird in der RPM-Datenbank aufgeführt. Wenn Sie ein Quellpaket "installieren", wird dem System nur der Quellcode hinzugefügt.

Die folgenden Verzeichnisse müssen für `rpm` und `rpmbuild` in `/usr/src/packages` vorhanden sein (es sei denn, Sie haben spezielle Einstellungen in einer Datei, wie `/etc/rpmrc`, festgelegt):

`SOURCES`
: für die originalen Quellen (`.tar.bz2` oder `.tar.gz` files, etc.) und für die distributionsspezifischen Anpassungen (meistens `.diff`- oder `.patch`-Dateien)

`SPECS`
: für die *.spec*-Dateien, die ähnlich wie Meta-Makefiles den *build*-Prozess steuern

`BUILD`
: Alle Quellen in diesem Verzeichnis werden entpackt, gepatcht und kompiliert.

`RPMS`
: Speicherort der fertigen Binärpakete

`SRPMS`
: Speicherort der Quell-RPMs

Wenn Sie ein Quellpaket mit YaST installieren, werden alle notwendigen Komponenten in `/usr/src/packages` installiert: die Quellen und Anpassungen in `SOURCES` und die relevanten `.spec`-Dateien in `SPECS`.

WARNUNG

Experimentieren Sie nicht mit Systemkomponenten (`glibc`, `rpm`, `sysvinit` usw.), da Sie damit die Funktionstüchtigkeit Ihres Systems aufs Spiel setzen.

Das folgende Beispiel verwendet das `wget.src.rpm`-Paket. Nach dem Installieren des Pakets mit YaST sollten Sie über Dateien ähnlich der in folgender Liste verfügen:

```
/usr/src/packages/SOURCES/nops_doc.diff
/usr/src/packages/SOURCES/toplev_destdir.diff
/usr/src/packages/SOURCES/wget-1.9.1+ipvmisc.patch
/usr/src/packages/SOURCES/wget-1.9.1-brokentime.patch
/usr/src/packages/SOURCES/wget-1.9.1-passive_ftp.diff
/usr/src/packages/SOURCES/wget-LFS-20040909.tar.bz2
/usr/src/packages/SOURCES/wget-wrong_charset.patch
/usr/src/packages/SPECS/wget.spec
```

Mit `rpmbuild -b X /usr/src/packages/SPECS/wget.spec` wird die Kompilierung gestartet. *X* ist ein Platzhalter für verschiedene Stufen des build-Prozesses (Einzelheiten siehe in `--help` oder der RPM-Dokumentation). Nachfolgend wird nur eine kurze Erläuterung gegeben:

`-bp`
: Bereiten Sie Quellen in `/usr/src/packages/BUILD` vor: entpacken und patchen.

`-bc`
: Wie `-bp`, jedoch zusätzlich kompilieren.

`-bi`
: Wie `-bp`, jedoch zusätzlich die erstellte Software installieren. Vorsicht: Wenn das Paket die Funktion BuildRoot nicht unterstützt, ist es möglich, dass Konfigurationsdateien überschrieben werden.

`-bb`
: Wie `-bi`, jedoch zusätzlich das Binärpaket erstellen. Nach erfolgreicher Kompilierung sollte das Binärpaket in `/usr/src/packages/RPMS` sein.

`-ba`
: Wie `-bb`, jedoch zusätzlich den Quell-RPM erstellen. Nach erfolgreicher Kompilierung sollte dieses in `/usr/src/packages/RPMS` liegen.

`--short-circuit`
: Einige Schritte überspringen.

Der erstellte Binär-RPM kann nun mit `rpm -i` oder vorzugsweise mit `rpm -U` erstellt werden. Durch die Installation mit `rpm` wird er in die RPM-Datenbank aufgenommen.

4.2.7 Kompilieren von RPM-Pakten mit "build"

Bei vielen Paketen besteht die Gefahr, dass während der Erstellung ungewollt Dateien in das laufende System kopiert werden. Um dies zu vermeiden, können Sie `build` verwenden, das eine definierte Umgebung herstellt, in der das Paket erstellt wird. Zum

Aufbau dieser chroot-Umgebung muss dem `build`-Skript ein kompletter Paketbaum zur Verfügung stehen. Dieser kann auf Festplatte, über NFS oder auch von DVD bereitgestellt werden. Legen Sie die Position mit `build --rpms` *`Verzeichnis`* fest. Im Unterschied zu `rpm` sucht der Befehl `build` die SPEC-Datei im Quellverzeichnis. Wenn Sie, wie im obigen Beispiel, wget neu erstellen möchten und die DVD unter `/media/dvd` im System eingehängt ist, verwenden Sie als Benutzer `root` folgende Befehle:

```
cd /usr/src/packages/SOURCES/
mv ../SPECS/wget.spec .
build --rpms /media/dvd/suse/ wget.spec
```

Anschließend wird in `/var/tmp/build-root` eine minimale Umgebung eingerichtet. Das Paket wird in dieser Umgebung erstellt. Danach befinden sich die resultierenden Pakete in `/var/tmp/build-root/usr/src/packages/RPMS`.

Das `build`-Skript bietet eine Reihe zusätzlicher Optionen. Beispielsweise können Sie das Skript veranlassen, Ihre eigenen RPMs bevorzugt zu verwenden, die Initialisierung der build-Umgebung auszulassen oder den Befehl `rpm` auf eine der oben erwähnten Stufen zu beschränken. Weitere Informationen erhalten Sie über `build --help` oder die Manualpage `build`.

4.2.8 Werkzeuge für RPM-Archive und die RPM-Datenbank

Midnight Commander (`mc`) kann den Inhalt von RPM-Archiven anzeigen und Teile daraus kopieren. Archive werden als virtuelle Dateisysteme dargestellt und bieten alle üblichen Menüoptionen von Midnight Commander. Zeigen Sie den `HEADER` mit F3 an. Zeigen Sie die Archivstruktur mit den Cursortasten und der Eingabetaste an. Kopieren Sie Archivkomponenten mit F5.

KDE bietet das Werkzeug kpackage als Front-End für `rpm` an. Ein Paket-Manager mit allen Funktionen ist als YaST-Modul verfügbar (siehe Kapitel 9, *Installieren bzw. Entfernen von Software* (↑*Bereitstellungshandbuch*)).

5 Bash-Shell und Bash-Skripte

Heutzutage werden zunehmend Computer mit einer grafischen Bedienoberfläche (GUI) wie KDE oder GNOME verwendet. Diese bieten zwar viele Funktionen, jedoch ist ihre Verwendung beschränkt, was automatische Aufgaben angeht. Shells sind eine gute Ergänzung für GUIs, und dieses Kapitel gibt Ihnen einen Überblick über einige Aspekte von Shells, in diesem Fall die Bash-Shell.

5.1 Was ist "die Shell"?

Traditionell handelt es sich bei *der* Shell um Bash (Bourne again Shell). Wenn in diesem Kapitel die Rede von "der Shell" ist, ist die Bash-Shell gemeint. Neben der Bash-Shell gibt es noch weitere Shells mit anderen Funktionen und Merkmalen. Wenn Sie weitere Informationen über andere Shells wünschen, suchen Sie in YaST nach *shell*.

5.1.1 Die Bash-Konfigurationsdateien

Eine Shell lässt sich als Folgendes aufrufen:

1. Als interative Login-Shell Diese wird zum Anmelden bei einem Computer durch den Aufruf von Bash mit der Option `--login` verwendet oder beim Anmelden an einem entfernten Computer mit SSH.

2. Als "gewöhnliche", interaktive Shell. Dies ist normalerweise beim Starten von xterm, konsole oder ähnlichen Tools der Fall.

3. Als nicht-interaktive Shell. Dies wird beim Aufrufen eines Shell-Skripts in der Kommandozeile verwendet.

Abhängig vom verwendeten Shell-Typ werden unterschiedliche Konfigurationsdateien gelesen. Die folgenden Tabellen zeigen die Login- und Nicht-Login-Shell-Konfigurationsdateien.

Tabelle 5.1 *Bash-Konfigurationsdateien für Login-Shells*

Datei	Beschreibung
`/etc/profile`	Bearbeiten Sie diese Datei nicht, andernfalls können Ihre Änderungen bei Ihrem nächsten Update zerstört werden.
`/etc/profile.local`	Verwenden Sie diese Datei, wenn Sie `/etc/profile` erweitern
`/etc/profile.d/`	Enthält systemweite Konfigurationsdateien für bestimmte Programme
`~/.profile`	Fügen Sie hier benutzerspezifische Konfigurationsdaten für Login-Shells ein.

Tabelle 5.2 *Bash-Konfigurationsdateien für Nicht-Login-Shells*

`/etc/bash.bashrc`	Bearbeiten Sie diese Datei nicht, andernfalls können Ihre Änderungen bei Ihrem nächsten Update zerstört werden.
`/etc/bash.bashrc.local`	Verwenden Sie diese Datei, um Ihre systemweiten Änderungen nur für die Bash-Shell einzufügen.
`~/bashrc`	Fügen Sie hier benutzerspezifische Konfigurationsdaten ein.

Daneben verwendet die Bash-Shell einige weitere Dateien:

Tabelle 5.3 *Besondere Dateien für die Bash-Shell*

Datei	Beschreibung
`~/.bash_history`	Enthält eine Liste aller Kommandos, die Sie eingegeben haben.
`~/.bash_logout`	Wird beim Abmelden verwendet.

5.1.2 Die Verzeichnisstruktur

Die folgende Tabelle bietet eine kurze Übersicht über die wichtigsten Verzeichnisse der höheren Ebene auf einem Linux-System. Ausführlichere Informationen über die Verzeichnisse und wichtige Unterverzeichnisse erhalten Sie in der folgenden Liste.

Tabelle 5.4 *Überblick über eine Standardverzeichnisstruktur*

Verzeichnis	Inhalt
`/`	Root-Verzeichnis - Startpunkt der Verzeichnisstruktur.
`/bin`	Grundlegende binäre Dateien, z. B. Befehle, die der Systemadministrator und normale Benutzer brauchen. Enthält gewöhnlich auch die Shells, z. B. Bash.
`/boot`	Statische Dateien des Bootloaders.
`/dev`	Erforderliche Dateien für den Zugriff auf Host-spezifische Geräte.
`/etc`	Host-spezifische Systemkonfigurationsdateien.
`/home`	Enthält die Home-Verzeichnisse aller Benutzer, die ein Konto auf dem System haben. Nur das Home-Verzeichnis von `root` befindet sich nicht unter `/home`, sondern unter `/root`.

Verzeichnis	Inhalt
/lib	Grundlegende freigegebene Bibliotheken und Kernel-Module.
/media	Einhängepunkte für Wechselmedien.
/mnt	Einhängepunkt für das temporäre Einhängen eines Dateisystems.
/opt	Add-On-Anwendungssoftwarepakete.
/root	Home-Verzeichnis für den Superuser root.
/sbin	Grundlegende Systembinärdateien.
/srv	Daten für Dienste, die das System bereitstellt.
/tmp	Temporäre Dateien.
/usr	Sekundäre Hierarchie mit Nur-Lese-Daten.
/var	Variable Daten wie Protokolldateien..
/windows	Nur verfügbar, wenn sowohl Microsoft Windows* als auch Linux auf Ihrem System installiert ist. Enthält die Windows-Daten.

Die folgende Liste bietet detailliertere Informationen und bietet einige Beispiele für die Dateien und Unterverzeichnisse, die in den Verzeichnissen gefunden werden können:

/bin
: Enthält die grundlegenden Shell-Befehle, die root und andere Benutzer verwenden können. Zu diesen Kommandos gehören ls, mkdir, cp, mv, rm und rmdir. /bin enthält auch Bash, die Standard-Shell in SUSE Linux Enterprise Server.

`/boot`
: Enthält Daten, die zum Booten erforderlich sind, z. B. den Bootloader, den Kernel und andre Daten, die verwendet werden, bevor der Kernel mit der Ausführung von Programmen im Benutzermodus beginnt.

`/dev`
: Enthält Gerätedateien, die Hardware-Komponenten darstellen.

`/etc`
: Enthält lokale Konfigurationsdateien, die den Betrieb von Programmen wie das X Window System steuern können. Das Unterverzeichnis `/etc/init.d` enthält Skripten, die während des Bootvorgangs ausgeführt werden.

`/home/`*`Benutzername`*
: Enthält die privaten Daten aller Benutzer, die ein Konto auf dem System haben. Die Dateien, die hier gespeichert sind, können nur durch den Besitzer oder den Systemadministrator geändert werden. Standardmäßig befinden sich hier Ihr E-Mail-Verzeichnis und Ihre persönliche Desktopkonfiguration in Form von verborgenen Dateien und Verzeichnissen. KDE-Benutzer finden die persönlichen Konfigurationsdaten für den Desktop unter `.kde` bzw. `.kde4`, GNOME-Benutzer unter `.gconf`.

ANMERKUNG: Home-Verzeichnis in einer Netzwerkumgebung

Wenn Sie in einer Netzwerkumgebung arbeiten, kann Ihr Home-Verzeichnis einem von `/home` abweichenden Verzeichnis zugeordnet sein.

`/lib`
: Enthält grundlegende freigegebene Bibliotheken, die zum Booten des Systems und zur Ausführung der Befehle im Root-Dateisystem erforderlich sind. Freigegebene Bibliotheken entsprechen in Windows DLL-Dateien.

`/media`
: Enthält Einhängepunkte für Wechselmedien, z. B. CD-ROMs, USB-Sticks und Digitalkameras (sofern sie USB verwenden). `Unter`/media sind beliebige Laufwerktypen gespeichert, mit Ausnahme der Festplatte Ihres Systems. Sobald Ihr Wechselmedium eingelegt bzw. mit dem System verbunden und eingehängt wurde, können Sie von hier darauf zugreifen.

`/mnt`
: Dieses Verzeichnis bietet einen Einhängepunkt für ein temporär eingehängtes Dateisystem. `root` kann hier Dateisysteme einhängen.

`/opt`
: Reserviert für die Installation zusätzlicher Software. Hier finden Sie Software- und größere Addon-Programmpakete. KDE3 befindet sich hier, während KDE4 und GNOME nach `/usr` verschoben wurden.

`/root`
: Home-Verzeichnis für den Benutzer `root`. Hier befinden sich persönliche Daten von " `root`".

`/sbin`
: Wie durch das `s` angegeben, enthält dieses Verzeichnis Dienstprogramme für den Superuser. `/sbin` enthält Binärdateien, die zusätzlich zu den Dateien in `/bin` wesentlich für Booten und Wiederherstellen des Systems erforderlich sind.

`/srv`
: Enhält Daten für Dienste, die das System bereitstellt, z. B. FTP und HTTP.

`/tmp`
: Dieses Verzeichnis wird von Programmen benutzt, die eine temporäre Speicherung von Dateien verlangen.

`/usr`
: `/usr` hat nichts mit Benutzern ("user") zu tun, sondern ist das Akronym für UNIX-Systemressourcen. Die Daten in `/usr` sind statische, schreibgeschützte Daten, die auf verschiedenen Hosts freigegeben sein können, die den Filesystem Hierarchy Standard (FHS) einhalten. Dieses Verzeichnis enthält alle Anwendungsprogramme und bildet eine sekundäre Hierarchie im Dateisystem. Dort befinden sich auch KDE4 und GNOME. `/usr` enthält eine Reihe von Unterverzeichnissen, z. B. `/usr/bin`, `/usr/sbin`, `/usr/local` und `/usr/share/doc`.

`/usr/bin`
: Enthält Programme, die für den allgemeinen Zugriff verfügbar sind.

`/usr/sbin`
: Enthält Programme, die für den Systemadministrator reserviert sind, z. B. Reparaturfunktionen.

`/usr/local`
: In diesem Verzeichnis kann der Systemadministrator lokale, verteilungsunabhängige Erweiterungen installieren.

`/usr/share/doc`
: Enthält verschiedene Dokumentationsdateien und die Versionshinweise für Ihr System. Im Unterverzeichnis `manual` befindet sich eine Online-Version dieses Handbuchs. Wenn mehrere Sprachen installiert sind, kann dieses Verzeichnis die Handbücher für verschiedene Sprachen enthalten.

  Im Verzeichnis `packages` befindet sich die Dokumentation zu den auf Ihrem System installierten Software-Paketen. Für jedes Paket wird ein Unterverzeichnis `/usr/share/doc/packages/`*`Paketname`* angelegt, das häufig README-Dateien für das Paket und manchmal Beispiele, Konfigurationsdateien oder zusätzliche Skripten umfasst.

  Wenn HOWTOs (Verfahrensbeschreibungen) auf Ihrem System installiert sind, enhält `/usr/share/doc` auch das Unterverzeichnis `howto` mit zusätzlicher Dokumentation zu vielen Aufgaben bei Setup und Betrieb von Linux-Software.

`/var`
: Während `/usr` statische, schreibgeschützte Daten enthält, ist `/var` für Daten, die während des Systembetriebs geschrieben werden und daher variabel sind, z. B. Protokolldateien oder Spooling-Daten. Beispielsweise befinden sich die Protokolldateien Ihres Systems in `/var/log/messages` (nur für "`root`" zugreifbar).

5.2 Schreiben von Shell-Skripten

Shell-Skripte bieten eine bequeme Möglichkeit, alle möglichen Aufgaben zu erledigen: Erfassen von Daten, Suche nach einem Wort oder Begriff in einem Text und viele andere nützliche Dinge. Das folgende Beispiel zeigt ein kleines Shell-Skript, das einen Text druckt:

Beispiel 5.1 *Ein Shell-Skript, das einen Text druckt*

```
#!/bin/sh ❶
# Output the following line: ❷
echo "Hello World" ❸
```

❶ Die erste Zeile beginnt mit den *Shebang*-Zeichen (`#!`), das darauf hinweist, dass es sich bei dieser Datei um ein Skript handelt. Das Skript wird mit dem Interpreter ausgeführt, der nach dem Shebang angegeben ist, in diesem Fall mit `/bin/sh`.

❷ Die zweite Zeile ist ein Kommentar, der mit dem Hash-Zeichen beginnt. Es wird empfohlen, schwierige Zeilen zu kommentieren, damit ihre Bedeutung auch später klar ist.

❸ Die dritte Zeile verwendet das integrierte Kommando `echo`, um den entsprechenden Text zu drucken.

Bevor Sie dieses Skript ausführen können, müssen einige Voraussetzungen erfüllt sein:

1. Jedes Skript muss eine Shebang-Zeile enthalten. (Dies ist im obigen Beispiel bereits der Fall.) Wenn ein Skript diese Zeile nicht enthält, müssen Sie den Interpreter selbst aufrufen.

2. Sie können das Skript an beliebiger Stelle speichern. Jedoch empfiehlt es sich, es in einem Verzeichnis zu speichern, in dem die Shell danach sucht. Der Suchpfad in einer Shell wird durch die Umgebungsvariable `PATH` bestimmt. Speichern Sie sie beispielsweise im Verzeichnis `~/bin/` unter dem Namen `hello.sh`.

3. Das Skript muss zum Ausführen von Dateien berechtigt sein. Stellen Sie die Berechtigungen mit dem folgenden Kommando ein:

   ```
   chmod +x ~/bin/hello.sh
   ```

Wenn die obigen Voraussetzungen erfüllt sind, können Sie das Skript mit `~/bin/hello.sh` oder `hello.sh` ausführen. Der erste Aufruf verwendet einen absoluten Pfad, während der zweite nach dem Kommando in dem Verzeichnis sucht, das die Umgebungsvariable `PATH` angibt.

5.3 Umlenken von Kommandoereignissen

Jedes Kommando kann drei Kanäle für Eingabe oder Ausgabe verwenden:

- **Standardausgabe** Dies ist der Standardausgabe-Kanal. Immer wenn ein Kommando eine Ausgabe erzeugt, verwendet es den Standardausgabe-Kanal.
- **Standardeingabe** Wenn ein Kommando Eingaben von Benutzern oder anderen Kommandos benötigt, verwendet es diesen Kanal.
- **Standardfehler** Kommandos verwenden diesen Kanal zum Melden von Fehlern.

Zum Umlenken dieser Kanäle bestehen folgende Möglichkeiten:

`Kommando > Datei`
: Speichert die Ausgabe des Kommandos in eine Datei; eine etwaige bestehende Datei wird gelöscht. Beispielsweise schreibt das Kommando `ls` seine Ausgabe in die Datei `listing.txt`:

```
ls > listing.txt
```

`Kommando >> Datei`
: Hängt die Ausgabe des Kommandos an eine Datei an. Beispielsweise hängt das Kommando `ls` seine Ausgabe an die Datei `listing.txt` an:

```
ls >> listing.txt
```

`Kommando < Datei`
: Liest die Datei als Eingabe für das angegebene Kommando. Beispielsweise liest das Kommando `read` den Inhalt der Datei in eine Variable ein:

```
read a < foo
```

`Kommando1 | Kommando2`
: Leitet die Ausgabe des linken Kommandos als Eingabe für das rechte Kommando um.

Jeder Kanal verfügt über einen *Dateideskriptor*: 0 (Null) für Standardeingabe, 1 für Standardausgabe und 2 für Standardfehler. Es ist zulässig, diesen Dateideskriptor vor einem <- oder >-Zeichen einzufügen. Beispielsweise sucht die folgende Zeile nach

einer Datei, die mit `foo` beginnt, aber seine Fehlermeldungen durch Umlenkung zu `/dev/null` unterdrückt:

```
find / -name "foo*" 2>/dev/null
```

5.4 Verwenden von Aliasen

Ein Alias ist ein Definitionskürzel für einen oder mehrere Kommandos. Die Syntax für einen Alias lautet:

```
alias NAME=DEFINITION
```

Beispielsweise definiert die folgende Zeile den Alias `lt`, der eine lange Liste ausgibt (Option `-l`), sie nach Änderungszeit sortiert (`-t`) und sie bei der Sortierung in umgekehrter Reihenfolge ausgibt (`-r`):

```
alias lt='ls -ltr'
```

Zur Anzeige aller Aliasdefinitionen verwenden Sie `alias`.

5.5 Verwenden von Variablen in der Bash-Shell

Eine Shell-Variable kann global oder lokal sein. Auf globale Variablen, z. B. Umgebungsvariablen, kann in allen Shells zugegriffen werden. Lokale Variablen sind hingegen nur in der aktuellen Shell sichtbar.

Verwenden Sie zur Anzeige von allen Umgebungsvariablen das Kommando `printenv`. Wenn Sie eine bestimmte Variable benötigen, fügen Sie den Namen Ihrer Variablen als Argument ein:

```
printenv PATH
```

Eine Variable kann auch über `echo` angezeigt werden:

```
echo $PATH
```

Damit wird die Variable `PATH` gedruckt. Verwenden Sie zum Festlegen einer lokalen Variablen einen Variablennamen, gefolgt vom Gleichheitszeichen und dem Wert für den Namen:

```
PROJECT="SLED"
```

Geben Sie keine Leerzeichen um das Gleichheitszeichen ein, sonst erhalten Sie einen Fehler. Verwenden Sie zum Setzen einer Umgebungsvariablen `export`:

```
export NAME="tux"
```

Zum Entfernen einer Variablen verwenden Sie `unset`:

```
unset NAME
```

Die folgende Tabelle enthält einige häufige Umgebungsvariablen, die Sie in Ihren Shell-Skripten verwenden können:

Tabelle 5.5 *Nützliche Umgebungsvariablen*

`HOME`	Home-Verzeichnis des aktuellen Benutzers
`HOST`	Aktueller Hostname
`LANG`	Wenn ein Werkzeug lokalisiert wird, verwendet es die Sprache aus dieser Umgebungsvariablen. Englisch kann auch auf `C` gesetzt werden.
`PATH`	Suchpfad der Shell, eine Liste von Verzeichnissen, die durch Doppelpunkte getrennt sind.
`PS1`	Gibt die normale Eingabeaufforderung an, die vor jedem Kommando angezeigt wird.
`PS2`	Gibt die sekundäre Eingabeaufforderung an, die beim Ausführen eines mehrzeiligen Kommandos angezeigt wird.
`PWD`	Aktuelles Arbeitsverzeichnis
`USER`	Aktueller Benutzer

5.5.1 Verwenden von Argumentvariablen

Wenn Sie beispielsweise über das Skript `foo.sh` verfügen, können Sie es wie folgt ausführen:

```
foo.sh "Tux Penguin" 2000
```

Für den Zugriff auf all diese Argumente, die an Ihr Skript übergeben werden, benötigen Sie Positionsparameter. Diese sind `$1` für das erste Argument, `$2` für das zweite usw. Sie können bis zu neun Parameter verwenden. Verwenden Sie `$0` zum Abrufen des Skriptnamens.

Das folgende Skript `foo.sh` gibt alle Argumente von 1 bis 4 aus:

```
#!/bin/sh
echo \"$1\" \"$2\" \"$3\" \"$4\"
```

Wenn Sie das Skript mit den obigen Argumenten ausführen, erhalten Sie Folgendes:

```
"Tux Penguin" "2000" "" ""
```

5.5.2 Verwenden der Variablenersetzung

Variablenersetzungen wenden beginnend von links oder rechts ein Schema auf den Inhalt einer Variablen an. Die folgende Liste enthält die möglichen Syntaxformen:

`${VAR#schema}`
: entfernt die kürzeste mögliche Übereinstimmung von links:

```
file=/home/tux/book/book.tar.bz2
echo ${file#*/}
home/tux/book/book.tar.bz2
```

`${VAR##schema}`
: entfernt die längste mögliche Übereinstimmung von links:

```
file=/home/tux/book/book.tar.bz2
echo ${file##*/}
book.tar.bz2
```

`${VAR%schema}`
: entfernt die kürzeste mögliche Übereinstimmung von rechts:

```
file=/home/tux/book/book.tar.bz2
echo ${file%.*}
/home/tux/book/book.tar
```

`${VAR%%schema}`
: entfernt die längste mögliche Übereinstimmung von rechts:

```
file=/home/tux/book/book.tar.bz2
echo ${file%%.*}
/home/tux/book/book
```

5.6 Gruppieren und Kombinieren von Kommandos

In den Shells können Sie Kommandos für bedingte Ausführung verketten und gruppieren. Jedes Kommando übergibt einen Endcode, der den Erfolg oder Misserfolg seiner Ausführung bestimmt. Wenn er 0 (Null) lautet, war das Kommando erfolgreich, alle anderen Codes bezeichnen einen Fehler, der spezifisch für das Kommando ist.

Die folgende Liste zeigt, wie sich Kommandos gruppieren lassen:

`Kommando1 ; Kommando2`
: führt die Kommandos in sequenzieller Reihenfolge aus. Der Endcode wird nicht geprüft. Die folgende Zeile zeigt den Inhalt der Datei mit `cat` an und gibt deren Dateieigenschaften unabhängig von deren Endcodes mit `ls` aus:

```
cat filelist.txt ; ls -l filelist.txt
```

`Kommando1 && Kommando2`
: führt das rechte Kommando aus, wenn das linke Kommando erfolgreich war (logisches UND). Die folgende Zeile zeigt den Inahlt der Datei an und gibt deren Dateieigenschaften nur aus, wenn das vorherige Kommando erfolgreich war (vgl. mit dem vorherigen Eintrag in dieser Liste):

```
cat filelist.txt && ls -l filelist.txt
```

`Kommando1 || Kommando2`
: führt das rechte Kommando aus, wenn das linke Kommando fehlgeschlagen ist (logisches ODER). Die folgende Zeile legt nur ein Verzeichnis in `/home/wilber/bar` an, wenn die Erstellung des Verzeichnisses in `/home/tux/foo` fehlgeschlagen ist:

```
mkdir /home/tux/foo || mkdir /home/wilber/bar
```

`funcname(){ ... }`
: erstellt eine Shell-Funktion. Sie können mithilfe der Positionsparameter auf ihre Argumente zugreifen. Die folgende Zeile definiert die Funktion `hello` für die Ausgabe einer kurzen Meldung:

```
hello() { echo "Hello $1"; }
```

Sie können diese Funktion wie folgt aufrufen:

```
hello Tux
```

Die Ausgabe sieht wie folgt aus:

```
Hello Tux
```

5.7 Arbeiten mit häufigen Ablaufkonstrukten

Zur Steuerung des Ablaufs von Ihrem Skript verfügt eine Shell über `while`-, `if`-, `for`- und `case`-Konstrukte.

5.7.1 Das Steuerungskommando "if"

`if` wird verwendet, um Ausdrücke zu prüfen. Beispielsweise testet der folgende Code, ob es sich beim aktuellen Benutzer um Tux handelt:

```
if test $USER = "tux" then
  echo "Hello Tux."
else
  echo "You are not Tux."
fi
```

Der Testausdruck kann so komplex oder einfach wie möglich sein. Der folgende Ausdruck prüft, ob die Datei `foo.txt` existiert:

```
if test -e /tmp/foo.txt
then
  echo "Found foo.txt"
fi
```

Weitere Ausdrücke finden Sie unter `http://www.cyberciti.biz/nixcraft/linux/docs/uniqlinuxfeatures/lsst/ch03sec02.html`.

5.7.2 Erstellen von Schleifen mit dem Kommando "for"

Mithilfe der for-Schleife können Sie Kommandos an einer Liste von Einträgen ausführen. Beispielsweise gibt der folgende Code einige Informationen über PNG-Dateien im aktuellen Verzeichnis aus:

```
for i in *.png; do
 ls -l $i
done
```

5.8 Weiterführende Informationen

Wichtige Informationen über die Bash-Shell finden Sie auf den man-Seiten zu `man sh`. Für weitere Informationen zu diesem Thema siehe die folgende Liste:

- `http://tldp.org/LDP/Bash-Beginners-Guide/html/index.html` – Bash Guide for Beginners (Bash-Anleitungen für Anfänger)
- `http://tldp.org/HOWTO/Bash-Prog-Intro-HOWTO.html` – BASH Programming - Introduction HOW-TO (BASH-Programmierung – Einführende schrittweise Anleitungen)
- `http://tldp.org/LDP/abs/html/index.html` – Advanced Bash-Scripting Guide (Bash-Skript-Anleitungen für Fortgeschrittene)
- `http://www.grymoire.com/Unix/Sh.html` – Sh - the Bourne Shell (Sh – die Bourne-Shell)

Teil II. System

32-Bit- und 64-Bit-Anwendungen in einer 64-Bit-Systemumgebung

6

SUSE® Linux Enterprise Server ist für mehrere 64-Bit-Plattformen verfügbar. Das bedeutet jedoch nicht unbedingt, dass alle enthaltenen Anwendungen bereits auf 64-Bit-Plattformen portiert wurden. SUSE Linux Enterprise Server unterstützt die Verwendung von 32-Bit-Anwendungen in einer 64-Bit-Systemumgebung. Dieses Kapitel gibt einen kurzen Überblick über die Implementierung dieser Unterstützung auf SUSE Linux Enterprise Server-64-Bit-Plattformen. Es wird erläutert, wie 32-Bit-Anwendungen ausgeführt werden (Laufzeitunterstützung) und wie 32-Bit-Anwendungen kompiliert werden sollten, damit sie sowohl in 32-Bit- als auch in 64-Bit-Systemanwendungen ausgeführt werden können. Außerdem finden Sie Informationen zur Kernel-API und es wird erläutert, wie 32-Bit-Anwendungen unter einem 64-Bit-Kernel ausgeführt werden können.

SUSE Linux Enterprise Server für die 64-Bit-Plattformen ia64, ppc64, System z und x86_64 ist so konzipiert, dass bestehende 32-Bit-Anwendungen sofort in der 64-Bit-Umgebung ausgeführt werden können. Die entsprechenden 32-Bit-Plattformen sind 86 für ia64, ppc für ppc64 und x86 für x86_64. Diese Unterstützung bedeutet, dass Sie weiterhin Ihre bevorzugten 32-Bit-Anwendungen verwenden können und nicht warten müssen, bis ein entsprechender 64-Bit-Port verfügbar ist. Das aktuelle ppc64-System führt die meisten Anwendungen im 32-Bit-Modus aus, es können aber auch 64-Bit-Anwendungen ausgeführt werden.

6.1 Laufzeitunterstützung

WICHTIG: Konflikte zwischen Anwendungsversionen

Wenn eine Anwendung sowohl für 32-Bit- als auch für 64-Bit-Umgebungen verfügbar ist, führt die parallele Installation beider Versionen zwangsläufig zu Problemen. Entscheiden Sie sich in diesen Fällen für eine der beiden Versionen und installieren und verwenden Sie nur diese.

Eine Ausnahme von dieser Regel ist PAM (Pluggable Authentication Modules). Während des Authentifizierungsprozesses verwendet SUSE Linux Enterprise Server PAM als Schicht für die Vermittlung zwischen Benutzer und Anwendung. Auf einem 64-Bit-Betriebssystem, das auch 32-Bit-Anwendungen ausführt, ist es stets erforderlich, beide Versionen eines PAM-Moduls zu installieren.

Für eine korrekte Ausführung benötigt jede Anwendung eine Reihe von Bibliotheken. Leider sind die Namen für die 32-Bit- und 64-Bit-Versionen dieser Bibliotheken identisch. Sie müssen auf andere Weise voneinander unterschieden werden.

Um die Kompatibilität mit der 32-Bit-Version aufrechtzuerhalten, werden die Bibliotheken am selben Ort im System gespeichert wie in der 32-Bit-Umgebung. Die 32-Bit-Version von `libc.so.6` befindet sich sowohl in der 32-Bit- als auch in der 64-Bit-Umgebung unter `/lib/libc.so.6`.

Alle 64-Bit-Bibliotheken und Objektdateien befinden sich in Verzeichnissen mit dem Namen `lib64`. Die 64-Bit-Objektdateien, die sich normalerweise unter `/lib` und `/usr/lib` befinden, werden nun unter `/lib64` und `/usr/lib64` gespeichert. Unter `/lib` und `/usr/lib` ist also Platz für die 32-Bit-Bibliotheken, sodass der Dateiname für beide Versionen unverändert bleiben kann.

Unterverzeichnisse von 32-Bit-Verzeichnissen namens `/lib`, deren Dateninhalt nicht von der Wortgröße abhängt, werden nicht verschoben. Das Schema entspricht LSB (Linux Standards Base) und FHS (File System Hierarchy Standard).

► **ipf:** Die 64-Bit-Bibliotheken für ia64 befinden sich in Standard-`lib`-Verzeichnissen. Es gibt weder ein Verzeichnis `lib64` noch ein Verzeichnis `lib32`. ia64 führt den 32-Bit-x86-Code unter einer Emulation aus. Eine Reihe von Basisbibliotheken wird unter `/emul/ia32-linux/lib` und `/emul/ia32-linux/usr/lib` installiert. ◄

6.2 Software-Entwicklung

Alle 64-Bit-Architekturen unterstützen die Entwicklung von 64-Bit-Objekten. Der Grad der Unterstützung für die 32-Bit-Kompilierung ist von der Architektur abhängig. Dies sind die verschiedenen Implementierungsoptionen für die Toolkette von GCC (GNU Compiler-Sammlung) und Binutils, die den Assembler `as` und den Linker `ld` umfassen:

Doppelarchitektur-Compiler
: Mit einer Doppelarchitektur-Entwicklungstoolkette können sowohl 32-Bit- als auch 64-Bit-Objekte erstellt werden. Das Kompilieren von 64-Bit-Objekten gehört bei fast allen Plattformen zum Standard. 32-Bit-Objekte können erstellt werden, wenn spezielle Flags verwendet werden. Dieses spezielle Flag ist `-m32` für GCC. Die Flags für die Binutils sind architekturabhängig, aber GCC überträgt die richtigen Flags an die Linker und Assembler. Zurzeit ist eine Doppelarchitektur-Entwicklungstoolkette für amd64 (unterstützt die Entwicklung von x86- und amd64-Anweisungen), System z und ppc64 vorhanden. 32-Bit-Objekte werden in der Regel auf der ppc64-Plattform erstellt. Zur Erstellung von 64-Bit-Objekten muss das Flag `-m64` verwendet werden.

Keine Unterstützung
: SUSE Linux Enterprise Server bietet keine Unterstützung für die direkte Entwicklung von 32-Bit-Software auf allen Plattformen. Zur Entwicklung von Anwendungen für x86 unter ia64 müssen Sie die entsprechende 32-Bit-Version von SUSE Linux Enterprise Server verwenden.

Alle Header-Dateien müssen in architekturunabhängiger Form geschrieben werden. Die installierten 32-Bit- und 64-Bit-Bibliotheken müssen eine API (Anwendungsprogrammschnittstelle) aufweisen, die zu den installierten Header-Dateien passt. Die normale SUSE Linux Enterprise Server-Umgebung wurde nach diesem Prinzip gestaltet. Bei manuell aktualisierten Bibliotheken müssen Sie diese Probleme selbst lösen.

6.3 Software-Kompilierung auf Doppelarchitektur-Plattformen

Um bei einer Doppelarchitektur Binärdateien für die jeweils andere Architektur zu entwickeln, müssen die entsprechenden Bibliotheken für die zweite Architektur

zusätzlich installiert werden. Diese Pakete heißen `rpmname-32bit` oder `rpmname-x86` (für ia64), wenn die zweite Architektur eine 32-Bit-Architektur ist, oder `rpmname-64bit`, wenn die zweite Architektur eine 64-Bit-Architektur ist. Außerdem benötigen Sie die entsprechenden Header und Bibliotheken aus den `rpmname-devel`-Paketen und die Entwicklungsbibliotheken für die zweite Architektur aus `rpmname-devel-32bit` oder `rpmname-devel-64bit`.

Zum Kompilieren eines Programms, das `libaio` auf einem System verwendet, dessen zweite Architektur eine 32-Bit-Architektur ist (x86_64 oder System z), benötigen Sie beispielsweise die folgenden RPMs:

libaio-32bit
: 32-Bit-Laufzeitpaket

libaio-devel-32bit
: Header und Bibliotheken für die 32-Bit-Entwicklung

libaio
: 64-Bit-Laufzeitpaket

libaio-devel
: Header und Bibliotheken für die 64-Bit-Entwicklung

Die meisten Open Source-Programme verwenden eine `autoconf`-basierte Programmkonfiguration. Um mit `autoconf` ein Programm für die zweite Architektur zu konfigurieren, überschreiben Sie die normalen Compiler- und Linker-Einstellungen von `autoconf`, indem Sie das Skript `configure` mit zusätzlichen Umgebungsvariablen ausführen.

Das folgende Beispiel bezieht sich auf ein x86_64-System mit x86 als zweiter Architektur. Beispiele für ppc64 mit ppc als Zweitarchitektur wären ähnlich. Dieses Beispiel gilt nicht für ia64-Systeme, wo Sie keine 32-Bit-Pakete erstellen können.

1. Verwenden Sie den 32-Bit-Compiler:

   ```
   CC="gcc -m32"
   ```

2. Weisen Sie den Linker an, 32-Bit-Objekte zu verarbeiten (verwenden Sie stets gcc als Linker-Frontend):

   ```
   LD="gcc -m32"
   ```

3 Legen Sie den Assembler für die Erstellung von 32-Bit-Objekten fest:

```
AS="gcc -c -m32"
```

4 Legen Sie fest, dass die Bibliotheken für `libtool` usw. aus `/usr/lib` stammen sollen:

```
LDFLAGS="-L/usr/lib"
```

5 Legen Sie fest, dass die Bibliotheken im Unterverzeichnis `lib` gespeichert werden sollen:

```
--libdir=/usr/lib
```

6 Legen Sie fest, dass die 32-Bit-X-Bibliotheken verwendet werden sollen:

```
--x-libraries=/usr/lib/xorg
```

Nicht alle diese Variablen werden für jedes Programm benötigt. Passen Sie sie an das entsprechende Programm an.

Ein Beispiel für einen `configure`-Aufruf zur Kompilierung einer nativen 32-Bit-Anwendung auf x86_64, ppc64 oder System z könnte wie folgt aussehen:

```
CC="gcc -m32"            \
LDFLAGS="-L/usr/lib;"  \
        .configure       \
          --prefix=/usr  \
          --libdir=/usr/lib
make
make install
```

6.4 Kernel-Spezifikationen

Die 64-Bit-Kernel für x86_64, ppc64 und System z bieten sowohl eine 64-Bit- als auch eine 32-Bit-Kernel-ABI (binäre Anwendungsschnittstelle). Letztere ist mit der ABI für den entsprechenden 32-Bit-Kernel identisch. Das bedeutet, dass die 32-Bit-Anwendung mit dem 64-Bit-Kernel auf die gleiche Weise kommunizieren kann wie mit dem 32-Bit-Kernel.

Die 32-Bit-Emulation der Systemaufrufe für einen 64-Bit-Kernel unterstützt nicht alle APIs, die von Systemprogrammen verwendet werden. Dies hängt von der Plattform

ab. Aus diesem Grund müssen einige wenige Anwendungen, wie beispielsweise `lspci`, auf Nicht-ppc64-Plattformen als 64-Bit-Programme kompiliert werden, damit sie ordnungsgemäß funktionieren. Auf IBM-System z sind nicht alle ioctls in der 32-Bit-Kernel-ABI verfügbar.

Ein 64-Bit-Kernel kann nur 64-Bit-Kernel-Module laden, die speziell für diesen Kernel kompiliert wurden. 32-Bit-Kernel-Module können nicht verwendet werden.

TIPP

Für einige Anwendungen sind separate, Kernel-ladbare Module erforderlich. Wenn Sie vorhaben, eine solche 32-Bit-Anwendung in einer 64-Bit-Systemumgebung zu verwenden, wenden Sie sich an den Anbieter dieser Anwendung und an Novell, um sicherzustellen, dass die 64-Bit-Version des Kernel-ladbaren Moduls und die kompilierte 32-Bit-Version der Kernel-API für dieses Modul verfügbar sind.

Booten und Konfigurieren eines Linux-Systems

7

Das Booten eines Linux-Systems umfasst mehrere unterschiedliche Komponenten. Die Hardware selbst wird vom BIOS initialisiert, das den Kernel mithilfe eines Bootloaders startet. Jetzt wird der Bootvorgang mit init und den Runlevels vollständig vom Betriebssystem gesteuert. Mithilfe des Runlevel-Konzepts können Sie Setups für die tägliche Verwendung einrichten und Wartungsaufgaben am System ausführen.

7.1 Der Linux-Bootvorgang

Der Linux-Bootvorgang besteht aus mehreren Phasen, von denen jede einer anderen Komponente entspricht. In der folgenden Liste werden der Bootvorgang und die daran beteiligten Komponenten kurz zusammengefasst.

1. **BIOS** Nach dem Einschalten des Computers initialisiert das BIOS den Bildschirm und die Tastatur und testet den Arbeitsspeicher. Bis zu dieser Phase greift der Computer nicht auf Massenspeichergeräte zu. Anschließend werden Informationen zum aktuellen Datum, zur aktuellen Uhrzeit und zu den wichtigsten Peripheriegeräten aus den CMOS-Werten geladen. Wenn die erste Festplatte und deren Geometrie erkannt wurden, geht die Systemkontrolle vom BIOS an den Bootloader über. Wenn das BIOS Netzwerk-Booting unterstützt, ist es auch möglich, einen Boot-Server zu konfigurieren, der den Bootloader bereitstellt. Auf x86-Systemen ist PXE-Boot erforderlich. Andere Architekturen verwenden meist das BOOTP-Protokoll, um den Bootloader abzurufen.

2. **Bootloader** Der erste physische 512 Byte große Datensektor der ersten Festplatte wird in den Arbeitsspeicher geladen und der *Bootloader*, der sich am Anfang dieses

Sektors befindet, übernimmt die Steuerung. Die vom Bootloader ausgegebenen Befehle bestimmen den verbleibenden Teil des Bootvorgangs. Aus diesem Grund werden die ersten 512 Byte auf der ersten Festplatte als *Master Boot Record* (MBR) bezeichnet. Der Bootloader übergibt die Steuerung anschließend an das eigentliche Betriebssystem, in diesem Fall an den Linux-Kernel. Weitere Informationen zu GRUB, dem Linux-Bootloader, finden Sie unter Kapitel 8, *Der Bootloader GRUB* (S. 85). Bei einem Netzwerk-Boot fungiert das BIOS als Bootloader. Es erhält das Image für den Start vom Boot-Server und starten dann das System. Dieser Vorgang ist vollständig unabhängig von den lokalen Festplatten.

3. **Kernel und "initramfs"** Um die Systemkontrolle zu übergeben, lädt das Startladeprogramm sowohl den Kernel als auch ein initiales RAM-basiertes Dateisystem (initramfs) in den Arbeitsspeicher. Der Inhalt des initramfs kann vom Kernel direkt verwendet werden. Das initramfs enthält eine kleine Programmdatei namens "init", die das Einhängen des eigentlichen Root-Dateisystems ausführt. Spezielle Hardware-Treiber für den Zugriff auf den Massenspeicher müssen in initramfs vorhanden sein. Weitere Informationen zu initramfs finden Sie unter Abschnitt 7.1.1, „initramfs“ (S. 67). Wenn das System über keine lokale Festplatte verfügt, muss initramfs das Root-Dateisystem für den Kernel bereitstellen. Dies kann mithilfe eines Netzwerkblockgeräts, wie iSCSI oder SAN, bewerkstelligt werden, es kann aber auch NFS als Root-Gerät eingesetzt werden.

4. **init on initramfs** Dieses Programm führt alle für das Einhängen des entsprechenden Root-Dateisystems erforderlichen Aktionen aus, z. B. das Bereitstellen der Kernel-Funktionalität für die erforderlichen Dateisystem- und Gerätetreiber der Massenspeicher-Controller mit udev. Nachdem das Root-Dateisystem gefunden wurde, wird es auf Fehler geprüft und eingehängt. Wenn dieser Vorgang erfolgreich abgeschlossen wurde, wird das initramfs bereinigt und das init-Programm wird für das Root-Dateisystem ausgeführt. Weitere Informationen zum init-Programm finden Sie in Abschnitt 7.1.2, „init on initramfs“ (S. 68). Weitere Informationen zu udev finden Sie in Kapitel 11, *Gerätemanagemet über dynamischen Kernel mithilfe von udev* (S. 143).

5. **init** Das init-Programm führt den eigentlichen Boot-Vorgang des Systems über mehrere unterschiedliche Ebenen aus und stellt dabei die unterschiedlichen Funktionalitäten zur Verfügung. Eine Beschreibung des init-Programms finden Sie in Abschnitt 7.2, „Der init-Vorgang“ (S. 70).

7.1.1 initramfs

initramfs ist ein kleines cpio-Archiv, das der Kernel auf einen RAM-Datenträger laden kann. Es stellt eine minimale Linux-Umgebung bereit, die das Ausführen von Programmen ermöglicht, bevor das eigentliche Root-Dateisystem eingehängt wird. Diese minimale Linux-Umgebung wird von BIOS-Routinen in den Arbeitsspeicher geladen und hat, abgesehen von ausreichend Arbeitsspeicher, keine spezifischen Hardware-Anforderungen. initramfs muss immer eine Programmdatei namens "init" zur Verfügung stellen, die das eigentliche init-Programm für das Root-Dateisystem ausführt, damit der Boot-Vorgang fortgesetzt werden kann.

Bevor das Root-Dateisystem eingehängt und das Betriebssystem gestartet werden kann, ist es für den Kernel erforderlich, dass die entsprechenden Treiber auf das Gerät zugreifen, auf dem sich das Root-Dateisystem befindet. Diese Treiber können spezielle Treiber für bestimmte Arten von Festplatten oder sogar Netzwerktreiber für den Zugriff auf ein Netzwerk-Dateisystem umfassen. Die erforderlichen Module für das Root-Dateisystem können mithilfe von init oder initramfs geladen werden. Nachdem die Module geladen wurden, stellt udev das initramfs mit den erforderlichen Geräten bereit. Später im Boot-Vorgang, nach dem Ändern des Root-Dateisystems, müssen die Geräte regeneriert werden. Dies erfolgt durch `boot.udev` mit dem Kommando `udevtrigger`.

Wenn in einem installierten System Hardwarekomponenten (z. B. Festplatten) ausgetauscht werden müssen und diese Hardware zur Boot-Zeit andere Treiber im Kernel erfordert, müssen Sie das initramfs aktualisieren. Sie gehen hierbei genauso vor, wie bei der Aktualisierung des Vorgängers initrd. Rufen Sie `mkinitrd` auf. Durch das Aufrufen von `mkinitrd` ohne Argumente wird ein initramfs erstellt. Durch das Aufrufen von `mkinitrd -R`wird ein initrd erstellt. In SUSE® Linux Enterprise Server werden die zu ladenden Module durch die Variable `INITRD_MODULES` in `/etc/sysconfig/kernel` angegeben. Nach der Installation wird diese Variable automatisch auf den korrekten Wert eingestellt. Die Module werden genau in der Reihenfolge geladen, in der sie in `INITRD_MODULES` angezeigt werden. Dies ist nur wichtig, wenn Sie sich auf die korrekte Einstellung der Gerätedateien `/dev/sd? verlassen.`. In bestehenden Systemen können Sie jedoch auch die Gerätedateien unter `/dev/disk/` verwenden, die in mehreren Unterverzeichnissen angeordnet sind (`by-id`, `by-path` und `by-uuid`) und stets dieselbe Festplatte darstellen. Dies ist auch während der Installation durch Angabe der entsprechenden Einhängeoption möglich.

WICHTIG: Aktualisieren von initramfs oder initrd

Der Bootloader lädt initramfs oder initrd auf dieselbe Weise wie den Kernel. Es ist nicht erforderlich, GRUB nach der Aktualisierung von initramfs oder initrd neu zu installieren, da GRUB beim Booten das Verzeichnis nach der richtigen Datei durchsucht.

7.1.2 init on initramfs

Der Hauptzweck von init unter initramfs ist es, das Einhängen des eigentlichen Root-Dateisystems sowie den Zugriff darauf vorzubereiten. Je nach aktueller Systemkonfiguration ist init für die folgenden Tasks verantwortlich.

Laden der Kernelmodule
: Je nach Hardwarekonfiguration sind für den Zugriff auf die Hardwarekomponenten des Computers (vor allem auf die Festplatte) spezielle Treiber erforderlich. Für den Zugriff auf das eigentliche Root-Dateisystem muss der Kernel die entsprechenden Dateisystemtreiber laden.

Bereitstellen von speziellen Blockdateien

: Der Kernel generiert Geräteereignisse für alle geladenen Module. udev verarbeitet diese Ereignisse und generiert die erforderlichen blockspezifischen Dateien auf einem RAM-Dateisystem im Verzeichnis `/dev`. Ohne diese speziellen Dateien wäre ein Zugriff auf das Dateisystem und andere Geräte nicht möglich.

Verwalten von RAID- und LVM-Setups
: Wenn Ihr System so konfiguriert ist, dass das Root-Dateisystem sich unter RAID oder LVM befindet, richtet init LVM oder RAID so ein, dass der Zugriff auf das Root-Dateisystem zu einem späteren Zeitpunkt erfolgt. Informationen über RAID und LVM finden Sie in Kapitel 15, *Fortgeschrittene Festplattenkonfiguration* (↑*Bereitstellungshandbuch*).

Verwalten von Netzwerkkonfigurationen
: Wenn Ihr System für die Verwendung eines Netzwerk-eingehängten Root-Dateisystems (über NFS eingehängt) konfiguriert ist, muss init sicherstellen, dass die entsprechenden Netzwerktreiber geladen und für den Zugriff auf das Root-Dateisystem eingerichtet werden.

Wenn sich das Dateisystem auf einem Netzwerkblockgerät, wie iSCSI oder SAN, befindet, wird die Verbindung zum Speicherserver ebenfalls vom initramfs eingerichtet.

Wenn init im Rahmen des Installationsvorgangs während des anfänglichen Boot-Vorgangs aufgerufen wird, unterscheiden sich seine Tasks von den zuvor beschriebenen:

Suchen des Installationsmediums
: Wenn Sie den Installationsvorgang starten, lädt Ihr Computer vom Installationsmedium einen Installationskernel und ein spezielles initrd mit dem YaST-Installationsprogramm. Das YaST-Installationsprogramm, das in einem RAM-Dateisystem ausgeführt wird, benötigt Daten über den Speicherort des Installationsmediums, um auf dieses zugreifen und das Betriebssystem installieren zu können.

Initiieren der Hardware-Erkennung und Laden der entsprechenden Kernelmodule
: Wie unter Abschnitt 7.1.1, „initramfs“ (S. 67) beschrieben, startet der Boot-Vorgang mit einem Mindestsatz an Treibern, die für die meisten Hardwarekonfigurationen verwendet werden können. init startet einen anfänglichen Hardware-Scan-Vorgang, bei dem die für die Hardwarekonfiguration geeigneten Treiber ermittelt werden. Die für den Boot-Vorgang benötigten Namen der Module werden in `INITRD_MODULES` in das Verzeichnis `/etc/sysconfig/kernel` geschrieben. Diese Namen werden verwendet, um ein benutzerdefiniertes initramfs zu erstellen, das zum Booten des Systems benötigt wird. Wenn die Module nicht zum Booten, sondern für coldplug benötigt werden, werden die Module in `/etc/sysconfig/hardware/hwconfig-*` geschrieben. Alle Geräte, die durch Konfigurationsdateien in diesem Verzeichnis beschrieben werden, werden beim Boot-Vorgang initialisiert.

Laden des Installations- oder Rettungssystems
: Sobald die Hardware erfolgreich erkannt und die entsprechenden Treiber geladen wurden und udev die speziellen Gerätedateien erstellt hat, startet init das Installationssystem, das das eigentliche YaST-Installationsprogramm bzw. das Rettungssystem enthält.

Starten von YaST
: init startet schließlich YaST, das wiederum die Paketinstallation und die Systemkonfiguration startet.

7.2 Der init-Vorgang

Das Programm init ist der Prozess mit der Prozess-ID 1. Es ist für die ordnungsgemäße Initialisierung des Systems verantwortlich. init wird direkt vom Kernel gestartet und widersteht dem Signal 9, das in der Regel Prozesse beendet. Alle anderen Programme werden entweder direkt von init oder von einem seiner untergeordneten Prozesse gestartet.

init wird zentral in der Datei `/etc/inittab` konfiguriert, in der auch die *Runlevel* definiert werden (siehe Abschnitt 7.2.1, „Runlevel“ (S. 70)). Diese Datei legt auch fest, welche Dienste und Daemons in den einzelnen Runlevels verfügbar sind. Je nach den Einträgen in `/etc/inittab` werden von init mehrere Skripten ausgeführt. Standardmäßig wird nach dem Booten als erstes Skript `/etc/init.d/boot` gestartet. Nach Abschluss der Systeminitialisierung ändert das System den Runlevel mithilfe des Skripts `/etc/init.d/rc` auf seinen Standard-Runlevel. Diese Skripten, die der Deutlichkeit halber als *init-Skripten* bezeichnet werden, befinden sich im Verzeichnis `/etc/init.d` (siehe Abschnitt 7.2.2, „Init-Skripten“ (S. 73)).

Der gesamte Vorgang des Startens und Herunterfahrens des Systems wird von init verwaltet. Von diesem Gesichtspunkt aus kann der Kernel als Hintergrundprozess betrachtet werden, dessen Aufgabe es ist, alle anderen Prozesse zu verwalten und die CPU-Zeit sowie den Hardwarezugriff entsprechend den Anforderungen anderer Programme anzupassen.

7.2.1 Runlevel

Unter Linux definieren *Runlevel*, wie das System gestartet wird und welche Dienste im laufenden System verfügbar sind. Nach dem Booten startet das System wie in `/etc/inittab` in der Zeile `initdefault` definiert. Dies ist in der Regel die Einstellung `3` oder `5`. Weitere Informationen hierzu finden Sie unter Tabelle 7.1, „Verfügbare Runlevel“ (S. 71). Alternativ kann der Runlevel auch zur Boot-Zeit (beispielsweise durch Einfügen der Runlevel-Nummer an der Eingabeaufforderung) angegeben werden. Alle Parameter, die nicht direkt vom Kernel ausgewertet werden können, werden an init übergeben. Zum Booten in Runlevel 3 fügen Sie der Booteingabeaufforderung einfach die Ziffer 3 hinzu.

Tabelle 7.1 *Verfügbare Runlevel*

Runlevel	Beschreibung
0	Systemstopp
S or 1	Einzelbenutzer-Modus
2	Lokaler Mehrbenutzer-Modus mit entferntem Netzwerk (NFS usw.)
3	Mehrbenutzer-Vollmodus mit Netzwerk
4	*Benutzerdefiniert*. Diese Option wird nicht verwendet, es sei denn, der Administrator konfiguriert diesen Runlevel.
5	Mehrbenutzer-Vollmodus mit Netzwerk und X-Display-Manager – KDM, GDM oder XDM
6	Systemneustart

WICHTIG: Runlevel 2 mit einer über NFS eingehängten Partition ist zu vermeiden

Sie sollten Runlevel 2 nicht verwenden, wenn Ihr System eine Partition, wie `/usr`, über NFS einhängt. Das System zeigt möglicherweise unerwartetes Verhalten, wenn Programmdateien oder Bibliotheken fehlen, da der NFS-Dienst in Runlevel 2 nicht zur Verfügung steht (lokaler Mehrbenutzer-Modus ohne entferntes Netzwerk).

Um die Runlevel während des laufenden Systembetriebs zu ändern, geben Sie `telinit` und die entsprechende Zahl als Argument ein. Dies darf nur von Systemadministratoren ausgeführt werden. In der folgenden Liste sind die wichtigsten Befehle im Runlevel-Bereich aufgeführt.

`telinit 1` oder `shutdown now`
: Das System wechselt in den *Einzelbenutzer-Modus*. Dieser Modus wird für die Systemwartung und administrative Aufgaben verwendet.

`telinit 3`
: Alle wichtigen Programme und Dienste (einschließlich Netzwerkprogramme und -dienste) werden gestartet und reguläre Benutzer können sich anmelden und mit dem System ohne grafische Umgebung arbeiten.

`telinit 5`
: Die grafische Umgebung wird aktiviert. Normalerweise wird ein Display-Manager, wie XDM, GDM oder KDM, gestartet. Wenn Autologin aktiviert ist, wird der lokale Benutzer beim vorausgewählten Fenster-Manager (GNOME, KDE oder einem anderem Fenster-Manager) angemeldet.

`telinit 0` oder `shutdown -h now`
: Das System wird gestoppt.

`telinit 6` oder `shutdown -r now`
: Das System wird gestoppt und anschließend neu gestartet.

Runlevel `5` ist Standard bei allen SUSE Linux Enterprise Server-Standardinstallationen. Die Benutzer werden aufgefordert, sich mit einer grafischen Oberfläche anzumelden, oder der Standardbenutzer wird automatisch angemeldet. Wenn der Standard-Runlevel `3` ist, muss das X Window System wie unter Kapitel 12, *Das X Window-System* (S. 159) beschrieben konfiguriert werden, bevor der Runlevel auf `5` geändert werden kann. Prüfen Sie anschließend, ob das System wie gewünscht funktioniert, indem Sie `telinit 5` eingeben. Wenn alles ordnungsgemäß funktioniert, können Sie mithilfe von YaST das Standard-Runlevel auf `5` setzen.

WARNUNG: Fehler in /etc/inittab können zu einem fehlerhaften Systemstart führen

Wenn `/etc/inittab` beschädigt ist, kann das System möglicherweise nicht ordnungsgemäß gebootet werden. Daher müssen Sie bei der Bearbeitung von `/etc/inittab` extrem vorsichtig sein. Lassen Sie init stets `/etc/inittab` mit dem Befehl `telinit q` neu lesen, bevor Sie den Rechner neu starten.

Beim Ändern der Runlevel geschehen in der Regel zwei Dinge. Zunächst werden Stopp-Skripten des aktuellen Runlevel gestartet, die einige der für den aktuellen Runlevel wichtigen Programme schließen. Anschließend werden die Start-Skripten des neuen Runlevel gestartet. Dabei werden in den meisten Fällen mehrere Programme gestartet. Beim Wechsel von Runlevel 3 zu 5 wird beispielsweise Folgendes ausgeführt:

1. Der Administrator (`root`) fordert init durch die Eingabe des Befehls `telinit 5` auf, zu einem anderen Runlevel zu wechseln.

2. init prüft den aktuellen Runlevel (`Runlevel`) und stellt fest, dass `/etc/init.d/rc` mit dem neuen Runlevel als Parameter gestartet werden soll.

3. Jetzt ruft `rc` die Stopp-Skripten des aktuellen Runlevel auf, für die es im neuen Runlevel keine Start-Skripten gibt. In diesem Beispiel sind dies alle Skripten, die sich in `/etc/init.d/rc3.d` (alter Runlevel war 3) befinden und mit einem `K` beginnen. Die Zahl nach `K` gibt die Reihenfolge an, in der die Skripten mit dem Parameter `stop` ausgeführt werden sollen, da einige Abhängigkeiten berücksichtigt werden müssen.

4. Die Start-Skripten des neuen Runlevel werden zuletzt gestartet. In diesem Beispiel befinden sie sich im Verzeichnis `/etc/init.d/rc5.d` und beginnen mit einem `S`. Auch hier legt die nach dem `S` angegebene Zahl die Reihenfolge fest, in der die Skripten gestartet werden sollen.

Bei dem Wechsel in denselben Runlevel wie der aktuelle Runlevel prüft init nur `/etc/inittab` auf Änderungen und startet die entsprechenden Schritte, z. B. für das Starten von `getty` auf einer anderen Schnittstelle. Dieselbe Funktion kann durch den Befehl `telinit q` erreicht werden.

7.2.2 Init-Skripten

Im Verzeichnis `/etc/init.d` gibt es zwei Skripttypen:

Skripten, die direkt von init ausgeführt werden
: Dies ist nur während des Boot-Vorgangs der Fall oder wenn das sofortige Herunterfahren des Systems initiiert wird (Stromausfall oder Drücken der Tastenkombination Strg + Alt + Entf). Bei IBM-System z-Systemen ist dies nur während des Boot-Vorgangs der Fall oder wenn das sofortige Herunterfahren des Systems initiiert wird (Stromausfall oder "Signalstilllegung"). Die Ausführung dieser Skripten ist in `/etc/inittab` definiert.

Skripten, die indirekt von init ausgeführt werden

Diese werden beim Wechsel des Runlevels ausgeführt und rufen immer das Master-Skript `/etc/init.d/rc` auf, das die richtige Reihenfolge der relevanten Skripten gewährleistet.

Sämtliche Skripten befinden sich im Verzeichnis `/etc/init.d`. Skripten, die während des Bootens ausgeführt werden, werden über symbolische Links aus `/etc/init.d/boot.d` aufgerufen. Skripten zum Ändern des Runlevels werden jedoch über symbolische Links aus einem der Unterverzeichnisse (`/etc/init.d/rc0.d` bis `/etc/init.d/rc6.d`) aufgerufen. Dies dient lediglich der Übersichtlichkeit und der Vermeidung doppelter Skripten, wenn diese in unterschiedlichen Runleveln verwendet werden. Da jedes Skript sowohl als Start- als auch als Stopp-Skript ausgeführt werden kann, müssen sie die Parameter `start` und `stop` erkennen. Die Skripten erkennen außerdem die Optionen `restart`, `reload`, `force-reload` und `status`. Diese verschiedenen Optionen werden in Tabelle 7.2, „Mögliche init-Skript-Optionen“ (S. 74) erläutert. Die von init direkt ausgeführten Skripten verfügen nicht über diese Links. Sie werden unabhängig vom Runlevel bei Bedarf ausgeführt.

Tabelle 7.2 *Mögliche init-Skript-Optionen*

Option	Beschreibung
`start`	Startet den Dienst.
`stop`	Stoppt den Dienst.
`restart`	Wenn der Dienst läuft, wird er gestoppt und anschließend neu gestartet. Wenn der Dienst nicht läuft, wird er gestartet.
`reload`	Die Konfiguration wird ohne Stoppen und Neustarten des Dienstes neu geladen.
`force-reload`	Die Konfiguration wird neu geladen, sofern der Dienst dies unterstützt. Anderenfalls erfolgt dieselbe Aktion wie bei dem Befehl `restart`.
`status`	Zeigt den aktuellen Status des Dienstes an.

Mithilfe von Links in den einzelnen Runlevel-spezifischen Unterverzeichnissen können Skripten mit unterschiedlichen Runleveln verknüpft werden. Bei der Installation oder Deinstallation von Paketen werden diese Links mithilfe des Programms "insserv" hinzugefügt oder entfernt (oder mithilfe von `/usr/lib/lsb/install_initd`, ein Skript, das dieses Programm aufruft). Weitere Informationen hierzu finden Sie auf der Manualpage "insserv(8)".

All diese Einstellungen können auch mithilfe des YaST-Moduls geändert werden. Wenn Sie den Status über die Kommandozeile prüfen, verwenden Sie das Werkzeug chkconfig, das auf der Manualpage "chkconfig(8)" beschrieben ist.

Im Folgenden finden Sie eine kurze Einführung in die zuerst bzw. zuletzt gestarteten Boot- und Stopp-Skripten sowie eine Erläuterung des Steuerskripten.

`boot`
: Werden ausgeführt, wenn das System direkt mit init gestartet wird. Es wird unabhängig vom gewählten Runlevel und nur einmalig ausgeführt. Dabei werden die Dateisysteme `/proc` und `/dev/pts` eingehängt und blogd (Boot Logging Daemon) wird aktiviert. Wenn das System nach einer Aktualisierung oder einer Installation das erste Mal gebootet wird, wird die anfängliche Systemkonfiguration gestartet.

  Der blogd-Daemon ist ein Dienst, der von boot und rc vor allen anderen Diensten gestartet wird. Er wird beendet, sobald die von diesen Skripten (die eine Reihe von Unterskripten ausführen, beispielsweise um spezielle Blockdateien verfügbar zu machen) ausgelösten Aktionen abgeschlossen sind. blogd schreibt alle Bildschirmausgaben in die Protokolldatei `/var/log/boot.msg`, jedoch nur wenn `/var` mit Schreib-/Lesezugriff eingehängt ist. Anderenfalls puffert blogd alle Bildschirmdaten, bis `/var` zur Verfügung steht. Weitere Informationen zu blogd erhalten Sie auf der Manualpage "blogd(8)".

  Das Skript `boot` ist zudem für das Starten aller Skripten in `/etc/init.d/boot.d` verantwortlich, deren Name mit `S` beginnt. Dort werden die Dateisysteme überprüft und bei Bedarf Loop-Devices konfiguriert. Außerdem wird die Systemzeit festgelegt. Wenn bei der automatischen Prüfung und Reparatur des Dateisystems ein Fehler auftritt, kann der Systemadministrator nach Eingabe des Root-Passworts eingreifen. Das zuletzt ausgeführte Skript ist `boot.local`.

`boot.local`
: Hier können Sie zusätzliche Befehle eingeben, die beim Booten ausgeführt werden sollen, bevor Sie zu einem Runlevel wechseln. Dieses Skript ist mit der `AUTOEXEC.BAT` in DOS-Systemen vergleichbar.

`halt`
: Dieses Skript wird nur beim Wechsel zu Runlevel 0 oder 6 ausgeführt. Es wird entweder als `halt` oder als `reboot` ausgeführt. Ob das System heruntergefahren oder neu gebootet wird, hängt davon ab, wie `halt` aufgerufen wird. Falls beim Herunterfahren Sonderkommandos benötigt werden, fügen Sie diese dem Skript `halt.local` hinzu.

`rc`
: Dieses Skript ruft die entsprechenden Stopp-Skripten des aktuellen Runlevels und die Start-Skripten des neu gewählten Runlevels auf. Wie das Skript `/etc/init.d/boot` wird auch dieses Skript über `/etc/inittab` mit dem gewünschten Runlevel als Parameter aufgerufen.

Sie können Ihre eigenen Skripten erstellen und diese problemlos in das oben beschriebene Schema integrieren. Anweisungen zum Formatieren, Benennen und Organisieren benutzerdefinierter Skripten finden Sie in den Spezifikationen von LSB und auf den man-Seiten von `init`, `init.d`, `chkconfig` und `insserv`. Weitere Informationen finden Sie zudem auf den man-Seiten zu `startproc` und `killproc`.

WARNUNG: Fehlerhafte init-Skripten können das System stoppen

Bei fehlerhaften init-Skripten kann es dazu kommen, dass der Computer hängt. Diese Skripten sollten mit großer Vorsicht bearbeitet werden und, wenn möglich, gründlich in der Mehrbenutzer-Umgebung getestet werden. Einige hilfreiche Informationen zu init-Skripten finden Sie in Abschnitt 7.2.1, „Runlevel“ (S. 70).

Sie erstellen ein benutzerdefiniertes init-Skript für ein bestimmtes Programm oder einen Dienst, indem Sie die Datei `/etc/init.d/skeleton` als Schablone verwenden. Speichern Sie eine Kopie dieser Datei unter dem neuen Namen und bearbeiten Sie die relevanten Programm- und Dateinamen, Pfade und ggf. weitere Details. Sie können das Skript auch mit eigenen Ergänzungen erweitern, sodass die richtigen Aktionen vom init-Prozess ausgelöst werden.

Der Block `INIT INFO` oben ist ein erforderlicher Teil des Skripts und muss bearbeitet werden. Weitere Informationen hierzu finden Sie unter Beispiel 7.1, „Ein minimaler INIT INFO-Block“ (S. 77).

Beispiel 7.1 *Ein minimaler INIT INFO-Block*

```
### BEGIN INIT INFO
# Provides:          FOO
# Required-Start:    $syslog $remote_fs
# Required-Stop:     $syslog $remote_fs
# Default-Start:     3 5
# Default-Stop:      0 1 2 6
# Description:       Start FOO to allow XY and provide YZ
### END INIT INFO
```

Geben Sie in der ersten Zeile des `INFO`-Blocks nach `Provides:` den Namen des Programms oder des Dienstes an, das bzw. der mit diesem Skript gesteuert werden soll. Geben Sie in den Zeilen `Required-Start:` und `Required-Stop:` alle Dienste an, die gestartet oder gestoppt werden müssen, bevor der Dienst selbst gestartet oder gestoppt wird. Diese Informationen werden später zum Generieren der Nummerierung der Skriptnamen verwendet, die in den Runlevel-Verzeichnissen enthalten sind. Geben Sie nach `Default-Start:` und `Default-Stop:` die Runlevel an, in denen der Dienst automatisch gestartet oder gestoppt werden soll. Geben Sie für `Description:` schließlich eine kurze Beschreibung des betreffenden Dienstes ein.

Um in den Runlevel-Verzeichnissen (`/etc/init.d/rc?.d/`) die Links auf die entsprechenden Skripten in `/etc/init.d/` zu erstellen, geben Sie den Befehl `insserv` *`neuer skriptname`* ein. Das Programm "insserv" wertet den `INIT INFO`-Header aus, um die erforderlichen Links für die Start- und Stopp-Skripten in den Runlevel-Verzeichnissen (`/etc/init.d/rc?.d/`) zu erstellen. Das Programm sorgt zudem für die richtige Start- und Stopp-Reihenfolge für die einzelnen Runlevel, indem es die erforderlichen Nummern in die Namen dieser Links aufnimmt. Wenn Sie ein grafisches Werkzeug bevorzugen, um solche Links zu erstellen, verwenden Sie den von YaST zur Verfügung gestellten Runlevel-Editor wie in Abschnitt 7.2.3, „Konfigurieren von Systemdiensten (Runlevel) mit YaST“ (S. 78) beschrieben.

Wenn ein in `/etc/init.d/` bereits vorhandenes Skript in das vorhandene Runlevel-Schema integriert werden soll, erstellen Sie die Links in den Runlevel-Verzeichnissen direkt mit insserv oder indem Sie den entsprechenden Dienst im Runlevel-Editor von YaST aktivieren. Ihre Änderungen werden beim nächsten Neustart wirksam und der neue Dienst wird automatisch gestartet.

Diese Links dürfen nicht manuell festgelegt werden. Wenn der `INFO`-Block Fehler enthält, treten Probleme auf, wenn `insserv` zu einem späteren Zeitpunkt für einen anderen Dienst ausgeführt wird. Der manuell hinzugefügte Dienst wird bei der nächsten Ausführung von `insserv` für dieses Skript entfernt.

7.2.3 Konfigurieren von Systemdiensten (Runlevel) mit YaST

Nach dem Start dieses YaST-Moduls mit *YaST* > *System* > *Systemdienste (Runlevel)* werden ein Überblick über alle verfügbaren Dienste sowie der aktuelle Status der einzelnen Dienste (deaktiviert oder aktiviert) angezeigt. Legen Sie fest, ob das Modul im *einfachen Modus* oder im *Expertenmodus* ausgeführt werden soll. Der vorgegebene *einfache Modus* sollte für die meisten Zwecke ausreichend sein. In der linken Spalte wird der Name des Dienstes, in der mittleren Spalte sein aktueller Status und in der rechten Spalte eine kurze Beschreibung angezeigt. Der untere Teil des Fensters enthält eine ausführlichere Beschreibung des ausgewählten Dienstes. Um einen Dienst zu aktivieren, wählen Sie ihn in der Tabelle aus und klicken Sie anschließend auf *Aktivieren*. Führen Sie die gleichen Schritte aus, um einen Dienst zu deaktivieren.

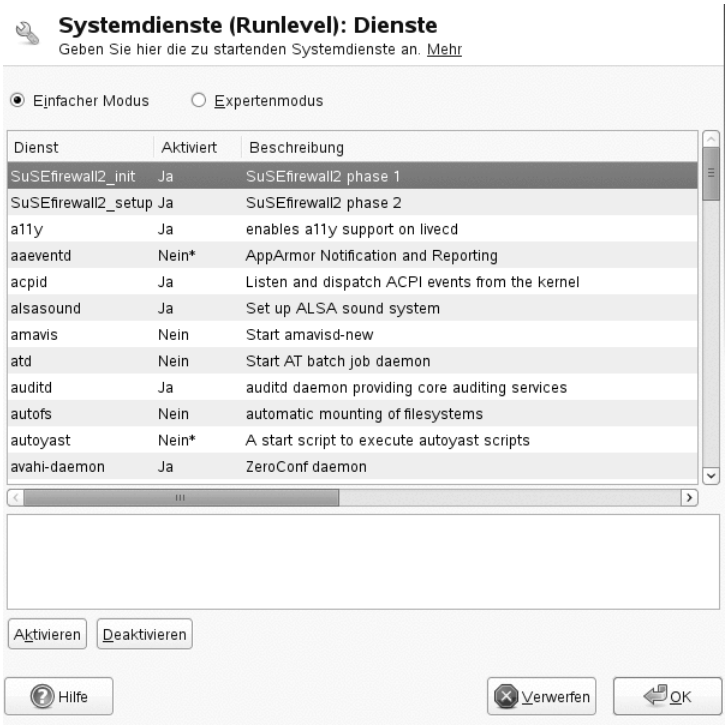
Die detaillierte Steuerung der Runlevel, in denen ein Dienst gestartet oder gestoppt bzw. die Änderung des vorgegebenen Runlevel erfolgt im *Expertenmodus*. Der aktuell vorgegebene Runlevel oder "initdefault" (der Runlevel, in den das System standardmäßig bootet) wird oben angezeigt. Das standardmäßige Runlevel eines SUSE Linux Enterprise Server-Systems ist in der Regel Runlevel 5 (Mehrbenutzer-Vollmodus mit Netzwerk und X). Eine geeignete Alternative kann Runlevel 3 sein (Mehrbenutzer-Vollmodus mit Netzwerk).

In diesem YaST-Dialogfeld können Sie ein Runlevel (wie unter Tabelle 7.1, „Verfügbare Runlevel“ (S. 71) aufgeführt) als neuen Standard wählen. Zudem können Sie mithilfe der Tabelle in diesem Fenster einzelne Dienste und Daemons aktivieren oder deaktivieren. In dieser Tabelle sind die verfügbaren Dienste und Daemons aufgelistet und es wird angezeigt, ob sie aktuell auf dem System aktiviert sind und wenn ja, für welche Runlevel. Nachdem Sie mit der Maus eine der Zeilen ausgewählt haben, klicken Sie auf die Kontrollkästchen, die die Runlevel (*B*, *0*, *1*, *2*, *3*, *5*, *6* und *S*) darstellen, um die Runlevel festzulegen, in denen der ausgewählte Dienst oder Daemon ausgeführt werden sollte. Runlevel 4 ist nicht definiert, um das Erstellen eines benutzerdefinierten Runlevel zu ermöglichen. Unterhalb der Tabelle wird eine kurze Beschreibung des aktuell ausgewählten Dienstes oder Daemons angezeigt.

WARNUNG: Fehlerhafte Runlevel-Einstellungen können das System beschädigen

Fehlerhafte Runlevel-Einstellungen können ein System unbrauchbar machen. Stellen Sie vor dem Anwenden der Änderungen sicher, dass Sie deren Auswirkungen kennen.

Abbildung 7.1 *Systemdienste (Runlevel)*


Systemdienste (Runlevel): Dienste
Geben Sie hier die zu startenden Systemdienste an. Mehr
Einfacher Modus
Expertenmodus
Dienst
Aktiviert
Beschreibung
SuSEfirewall2_init Ja SuSEfirewall2 phase 1
SuSEfirewall2_setup Ja SuSEfirewall2 phase 2
a11y Ja enables a11y support on livecd
aaeventd Nein* AppArmor Notification and Reporting
acpid Ja Listen and dispatch ACPI events from the kernel
alsasound Ja Set up ALSA sound system
amavis Nein Start amavisd-new
atd Nein Start AT batch job daemon
auditd Ja auditd daemon providing core auditing services
autofs Nein automatic mounting of filesystems
autoyast Nein* A start script to execute autoyast scripts
avahi-daemon Ja ZeroConf daemon
Aktivieren
Deaktivieren
Hilfe
Verwerfen
OK

Legen Sie mit den Optionen *"Start", "Anhalten" oder "Aktualisieren"* fest, ob ein Dienst aktiviert werden soll. *Status aktualisieren* prüft den aktuellen Status. *Mit "Übernehmen" oder "Zurücksetzen"* können Sie wählen, ob die Änderungen für das System angewendet werden sollen, oder ob die ursprünglichen Einstellungen wiederhergestellt werden sollen, die vor dem Starten des Runlevel-Editors wirksam waren. Mit *Verlassen* speichern Sie die geänderten Einstellungen.

7.3 Systemkonfiguration über /etc/sysconfig

Die Hauptkonfiguration von SUSE Linux Enterprise Server wird über die Konfigurationsdateien in `/etc/sysconfig` gesteuert. Die einzelnen Dateien in `/etc/sysconfig` werden nur von den Skripten gelesen, für die sie relevant sind. Dadurch wird gewährleistet, dass Netzwerkeinstellungen beispielsweise nur von netzwerkbezogenen Skripten analysiert werden.

Sie haben zwei Möglichkeiten, die Systemkonfiguration zu bearbeiten. Entweder verwenden Sie den YaST-Editor "sysconfig" oder Sie bearbeiten die Konfigurationsdateien manuell.

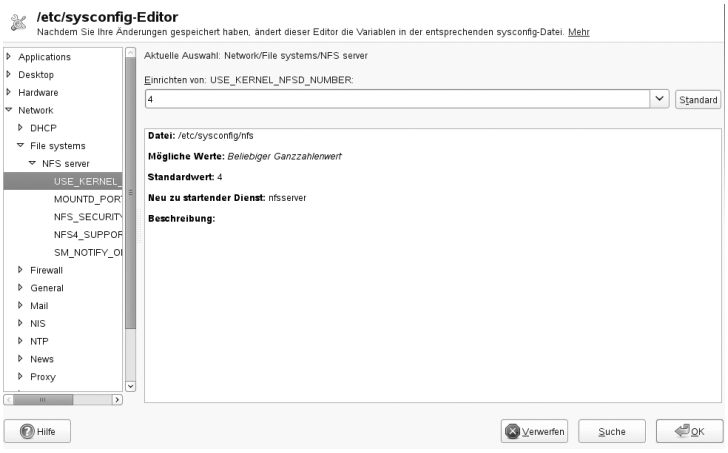
7.3.1 Ändern der Systemkonfiguration mithilfe des YaST-Editors "sysconfig"

Der YaST-Editor "sysconfig" bietet ein benutzerfreundliches Frontend für die Systemkonfiguration. Ohne den eigentlichen Speicherort der zu ändernden Konfigurationsvariablen zu kennen, können Sie mithilfe der integrierten Suchfunktion dieses Moduls den Wert der Konfigurationsvariable wie erforderlich ändern. YaST wendet diese Änderungen an, aktualisiert die Konfigurationen, die von den Werten in `sysconfig` abhängig sind, und startet die Dienste neu.

WARNUNG: Das Ändern von `/etc/sysconfig/*`-Dateien kann die Installation beschädigen

Sie sollten die Dateien `/etc/sysconfig`-Dateien nur bearbeiten, wenn Sie über ausreichende Sachkenntnisse verfügen. Das unsachgemäße Bearbeiten dieser Dateien kann zu schwerwiegenden Fehlern des Systems führen. Die Dateien in `/etc/sysconfig` enthalten einen kurzen Kommentar zu den einzelnen Variablen, der erklärt, welche Auswirkungen diese tatsächlich haben.

Abbildung 7.2 *Systemkonfiguration mithilfe des sysconfig-Editors*



Das YaST-Dialogfeld "sysconfig" besteht aus drei Teilen. Auf der linken Seite des Dialogfelds wird eine Baumstruktur aller konfigurierbaren Variablen angezeigt. Wenn Sie eine Variable auswählen, werden auf der rechten Seite sowohl die aktuelle Auswahl als auch die aktuelle Einstellung dieser Variable angezeigt. Unten werden in einem dritten Fenster eine kurze Beschreibung des Zwecks der Variable, mögliche Werte, der Standardwert und die Konfigurationsdatei angezeigt, aus der diese Variable stammt. In diesem Dialogfeld werden zudem Informationen dazu zur Verfügung gestellt, welche Konfigurationsskripten nach dem Ändern der Variable ausgeführt und welche neuen Dienste als Folge dieser Änderung gestartet werden. YaST fordert Sie auf, die Änderungen zu bestätigen und zeigt an, welche Skripten ausgeführt werden, wenn Sie *Verlassen* wählen. Außerdem können Sie die Dienste und Skripten auswählen, die jetzt übersprungen und zu einem späteren Zeitpunkt gestartet werden sollen. YaST wendet alle Änderungen automatisch an und startet alle von den Änderungen betroffenen Dienste neu, damit die Änderungen wirksam werden.

7.3.2 Manuelles Ändern der Systemkonfiguration

Gehen Sie wie folgt vor, um die Systemkonfiguration manuell zu ändern:

1. Melden Sie sich als `root` an.
2. Wechseln Sie mit `telinit 1` in den Einzelbenutzer-Modus (Runlevel 1).
3. Nehmen Sie die erforderlichen Änderungen an den Konfigurationsdateien in einem Editor Ihrer Wahl vor.

   Wenn Sie die Konfigurationsdateien in `/etc/sysconfig` nicht mit YaST ändern, müssen Sie sicherstellen, dass leere Variablenwerte durch zwei Anführungszeichen (`KEYTABLE=""`) gekennzeichnet sind, und Werte, die Leerzeichen enthalten, in Anführungszeichen gesetzt werden. Werte, die nur aus einem Wort bestehen, müssen nicht in Anführungszeichen gesetzt werden.
4. Führen Sie `SuSEconfig` aus, um sicherzustellen, dass die Änderungen wirksam werden.
5. Mit einem Kommando wie `telinit` *`default_runlevel`* stellen Sie den vorherigen Runlevel des Systems wieder her. Ersetzen Sie *`default_runlevel`* durch den vorgegebenen Runlevel des Systems. Wählen Sie `5`, wenn Sie in den Mehrbenutzer-Vollmodus mit Netzwerk und X zurückkehren möchten, oder wählen Sie `3`, wenn Sie lieber im Mehrbenutzer-Vollmodus mit Netzwerk arbeiten möchten.

Dieses Verfahren ist hauptsächlich beim Ändern von systemweiten Einstellungen, z. B. der Netzwerkkonfiguration, relevant. Für kleinere Änderungen ist der Wechsel in den Einzelbenutzer-Modus nicht erforderlich. In diesem Modus können Sie jedoch sicherstellen, dass alle von den Änderungen betroffenen Programme ordnungsgemäß neu gestartet werden.

TIPP: Konfigurieren der automatisierten Systemkonfiguration

Um die automatisierte Systemkonfiguration von SuSEconfig zu deaktivieren, setzen Sie die Variable `ENABLE_SUSECONFIG` in `/etc/sysconfig/`

`suseconfig` auf `no`. Wenn Sie den SUSE-Support für die Installation nutzen möchten, darf SuSEconfig nicht deaktiviert werden. Es ist auch möglich, die automatisierte Konfiguration teilweise zu deaktivieren.

8 Der Bootloader GRUB

In diesem Kapitel wird die Konfiguration von GRUB, dem in SUSE® Linux Enterprise Server verwendeten Bootloader, beschrieben. Zum Vornehmen der Einstellungen steht ein spezielles YaST-Modul zur Verfügung. Wenn Sie mit dem Bootvorgang unter Linux nicht vertraut sind, lesen Sie die folgenden Abschnitte, um einige Hintergrundinformationen zu erhalten. In diesem Kapitel werden zudem einige der Probleme, die beim Booten mit GRUB auftreten können, sowie deren Lösungen beschrieben.

ANMERKUNG: Kein GRUB auf Computern, die UEFI verwenden

GRUB wird routinemäßig auf Computern installiert, die mit einem traditionellen BIOS ausgestattet sind, bzw. auf UEFI (Unified Extensible Firmware Interface)-Computern, die ein kompatibles Supportmodul (Compatibility Support Module, CSM) verwenden. Auf UEFI-Computern ohne aktiviertes CSM wird automatisch `eLILO` installiert (vorausgesetzt, dass DVD1 erfolgreich gestartet wurde). Details finden Sie in der eLILO-Dokumentation unter `/usr/share/doc/packages/elilo/` auf Ihrem System.

Dieses Kapitel konzentriert sich auf das Bootmanagement und die Konfiguration des Bootloaders GRUB. Eine Übersicht über den Bootvorgang finden Sie in Kapitel 7, *Booten und Konfigurieren eines Linux-Systems* (S. 65). Ein Bootloader stellt die Schnittstelle zwischen dem Computer (BIOS) und dem Betriebssystem (SUSE Linux Enterprise Server) dar. Die Konfiguration des Bootloaders wirkt sich direkt auf das Starten des Betriebssystems aus.

In diesem Kapitel werden folgende Begriffe regelmäßig verwendet und daher ausführlicher beschrieben:

Master Boot Record
: Die Struktur des MBR ist durch eine vom Betriebssystem unabhängige Konvention definiert. Die ersten 446 Byte sind für Programmcode reserviert. Sie enthalten typischerweise einen Teil eines Bootloader-Programms oder eine Betriebssystemauswahl. Die nächsten 64 Byte bieten Platz für eine Partitionstabelle mit bis zu vier Einträgen. Die Partitionstabelle enthält Informationen zur Partitionierung der Festplatte und zu Dateisystemtypen. Das Betriebssystem benötigt diese Tabelle für die Verwaltung der Festplatte. Beim konventionellen generischen Code im MBR muss genau eine Partition als *aktiv* markiert sein. Die letzten beiden Byte müssen eine statische "magische Zahl" (AA55) enthalten. Ein MBR, der dort einen anderen Wert enthält, wird von einigen BIOS als ungültig und daher nicht zum Booten geeignet angesehen.

Bootsektoren
: Bootsektoren sind die jeweils ersten Sektoren der Festplattenpartitionen, außer bei der erweiterten Partition, die nur ein "Container" für andere Partitionen ist. Diese Bootsektoren reservieren 512 Byte Speicherplatz für Code, der ein auf dieser Partition befindliches Betriebssystem starten kann. Dies gilt für Bootsektoren formatierter DOS-, Windows- oder OS/2-Partitionen, die zusätzlich noch wichtige Basisdaten des Dateisystems enthalten. Im Gegensatz dazu sind Bootsektoren von Linux-Partitionen nach der Einrichtung eines anderen Dateisystems als XFS zunächst leer. Eine Linux-Partition ist daher nicht durch sich selbst bootfähig, auch wenn sie einen Kernel und ein gültiges root-Dateisystem enthält. Ein Bootsektor mit gültigem Code für den Systemstart trägt in den letzten 2 Byte dieselbe "magische" Zahl wie der MBR (`AA55`).

8.1 Booten mit GRUB

GRUB (Grand Unified Bootloader) besteht aus zwei Stufen. Stufe 1 (stage1) besteht aus 512 Byte und erfüllt lediglich die Aufgabe, die zweite Stufe des Bootloaders zu laden. Anschließend wird Stufe 2 (stage2) geladen. Diese Stufe enthält den Hauptteil des Bootloaders.

In einigen Konfigurationen gibt es eine zusätzliche Zwischenstufe 1.5, die Stufe 2 von einem geeigneten Dateisystem lokalisiert und lädt. Wenn diese Methode zur Verfügung steht, wird sie bei der Installation oder bei der anfänglichen Einrichtung von GRUB mit YaST standardmäßig gewählt.

stage2 kann auf zahlreiche Dateisysteme zugreifen. Derzeit werden Ext2, Ext3, ReiserFS, Minix und das von Windows verwendete DOS FAT-Dateisystem unterstützt. Bis zu einem gewissen Grad werden auch die von BSD-Systemen verwendeten , XFS, UFS und FFS unterstützt. Seit Version 0.95 kann GRUB auch von einer CD oder DVD booten, die das ISO 9660-Standarddateisystem nach der "El Torito"-Spezifikation enthält. GRUB kann noch vor dem Booten auf Dateisysteme unterstützter BIOS-Datenträgerlaufwerke (vom BIOS erkannte Disketten-, Festplatten-, CD- oder DVD-Laufwerke) zugreifen. Daher ist keine Neuinstallation des Bootmanagers nötig, wenn die Konfigurationsdatei von GRUB (`menu.lst`) geändert wird. Beim Booten des Systems liest GRUB die Menüdatei sowie die aktuellen Pfade und Partitionsdaten zum Kernel oder zur Initial RAM-Disk (`initrd`) neu ein und findet diese Dateien selbstständig.

Die eigentliche Konfiguration von GRUB basiert auf den im Folgenden beschriebenen drei Dateien:

`/boot/grub/menu.lst`
: Diese Datei enthält alle Informationen zu Partitionen oder Betriebssystemen, die mit GRUB gebootet werden können. Wenn diese Angaben nicht zur Verfügung stehen, muss der Benutzer in der GRUB-Kommandozeile das weitere Vorgehen angeben (siehe „Ändern von Menü-Einträgen während des Bootvorgangs“ (S. 92)).

`/boot/grub/device.map`
: Diese Datei übersetzt Gerätenamen aus der GRUB- und BIOS-Notation in Linux-Gerätenamen.

`/etc/grub.conf`
: Diese Datei enthält die Befehle, Parameter und Optionen, die die GRUB-Shell für das ordnungsgemäße Installieren des Bootloaders benötigt.

GRUB kann auf mehrere Weisen gesteuert werden. Booteinträge aus einer vorhandenen Konfiguration können im grafischen Menü (Eröffnungsbildschirm) ausgewählt werden. Die Konfiguration wird aus der Datei `menu.lst` geladen.

In GRUB können alle Bootparameter vor dem Booten geändert werden. Auf diese Weise können beispielsweise Fehler behoben werden, die beim Bearbeiten der Menüdatei aufgetreten sind. Außerdem können Bootbefehle über eine Art Eingabeaufforderung (siehe „Ändern von Menü-Einträgen während des Bootvorgangs“ (S. 92)) interaktiv eingegeben werden. &GRUB bietet die Möglichkeit, noch vor dem Booten die Position des Kernels und die Position von `initrd` zu ermitteln. Auf diese Weise können Sie

auch ein installiertes Betriebssystem booten, für das in der Konfiguration des Bootloaders noch kein Eintrag vorhanden ist.

GRUB ist in zwei Versionen vorhanden: als Bootloader und als normales Linux-Programm in `/usr/sbin/grub`. Dieses Programm wird als *GRUB-Shell* bezeichnet. Es stellt auf dem installierten System eine Emulation von GRUB bereit, die zum Installieren von GRUB oder zum Testen neuer Einstellungen verwendet werden kann. Die Funktionalität, GRUB als Bootloader auf einer Festplatte oder Diskette zu installieren, ist in Form der Befehle `install` und `setup` in GRUB integriert. Diese Befehle sind in der GRUB-Shell verfügbar, wenn Linux geladen ist.

8.1.1 Das GRUB-Bootmenü

Der grafische Eröffnungsbildschirm mit dem Bootmenü basiert auf der GRUB-Konfigurationsdatei `/boot/grub/menu.lst`, die alle Informationen zu allen Partitionen oder Betriebssystemen enthält, die über das Menü gebootet werden können.

Bei jedem Systemstart liest GRUB die Menüdatei vom Dateisystem neu ein. Es besteht also kein Bedarf, GRUB nach jeder Änderung an der Datei neu zu installieren. Mit dem YaST-Bootloader können Sie die GRUB-Konfiguration wie in Abschnitt 8.2, „Konfigurieren des Bootloaders mit YaST“ (S. 96) beschrieben ändern.

Die Menüdatei enthält Befehle. Die Syntax ist sehr einfach. Jede Zeile enthält einen Befehl, gefolgt von optionalen Parametern, die wie bei der Shell durch Leerzeichen getrennt werden. Einige Befehle erlauben aus historischen Gründen ein Gleichheitszeichen (=) vor dem ersten Parameter. Kommentare werden durch ein Rautezeichen (#) eingeleitet.

Zur Erkennung der Menüeinträge in der Menü-Übersicht, müssen Sie für jeden Eintrag einen Namen oder einen `title` vergeben. Der nach dem Schlüsselwort `title` stehende Text wird inklusive Leerzeichen im Menü als auswählbare Option angezeigt. Alle Befehle bis zum nächsten `title` werden nach Auswahl dieses Menüeintrags ausgeführt.

Der einfachste Fall ist die Umleitung zu Bootloadern anderer Betriebssysteme. Der Befehl lautet `chainloader` und das Argument ist normalerweise der Bootblock einer anderen Partition in der Blocknotation von GRUB. Beispiel:

```
chainloader (hd0,3)+1
```

Die Gerätenamen in GRUB werden in „Namenskonventionen für Festplatten und Partitionen“ (S. 89) beschrieben. Dieses Beispiel spezifiziert den ersten Block der vierten Partition auf der ersten Festplatte.

Mit dem Befehl `kernel` wird ein Kernel-Image angegeben. Das erste Argument ist der Pfad zum Kernel-Image auf einer Partition. Die restlichen Argumente werden dem Kernel in seiner Kommandozeile übergeben.

Wenn der Kernel nicht über die erforderlichen Treiber für den Zugriff auf die root-Partition verfügt oder ein aktuelles Linux-System mit erweiterten Hotplug-Funktionen verwendet wird, muss `initrd` mit einem separaten GRUB-Befehl angegeben werden, dessen einziges Argument der Pfad zur Datei `initrd` ist. Da die Ladeadresse von `initrd` in das geladene Kernel-Image geschrieben wird, muss der Befehl `initrd` auf den Befehl `kernel` folgen.

Der Befehl `root` vereinfacht die Angabe der Kernel- und initrd-Dateien. Das einzige Argument von `root` ist ein Gerät oder eine Partition. Allen Kernel-, `initrd`- oder anderen Dateipfaden, für die nicht explizit ein Gerät angegeben ist, wird bis zum nächsten `root`-Befehl das Gerät vorangestellt.

Am Ende jeden Menüeintrags steht implizit der `boot`-Befehl, sodass dieser nicht in die Menüdatei geschrieben werden muss. Wenn Sie GRUB jedoch interaktiv zum Booten verwenden, müssen Sie den `boot`-Befehl am Ende eingeben. Der Befehl selbst hat keine Argumente. Er führt lediglich das geladene Kernel-Image oder den angegebenen Chainloader aus.

Wenn Sie alle Menüeinträge geschrieben haben, müssen Sie einen Eintrag als `default` festlegen. Anderenfalls wird der erste Eintrag (Eintrag `0`) verwendet. Sie haben auch die Möglichkeit, ein Zeitlimit in Sekunden anzugeben, nach dem der default-Eintrag gebootet wird. `timeout` und `default` werden den Menüeinträgen in der Regel vorangestellt. Eine Beispieldatei finden Sie in „Beispiel einer Menüdatei“ (S. 90).

Namenskonventionen für Festplatten und Partitionen

Die von GRUB für Festplatten und Partitionen verwendeten Namenskonventionen unterscheiden sich von denen, die für normale Linux-Geräte verwendet werden. Sie sind der einfachen Plattennummerierung, die das BIOS durchführt, sehr ähnlich und die Syntax gleicht derjenigen, die in manchen BSD-Derivaten verwendet wird. In GRUB beginnt die Nummerierung der Partitionen mit null. Daher ist (`hd0,0`) die erste Parti-

tion auf der ersten Festplatte. Auf einem gewöhnlichen Desktop-Computer, bei dem eine Festplatte als Primary Master angeschlossen ist, lautet der entsprechende Linux-Gerätename `/dev/sda1`.

Die vier möglichen primären Partitionen haben die Partitionsnummern `0` bis `3`. Ab `4` werden die logischen Partitionen hochgezählt:

```
(hd0,0)   first primary partition of the first hard disk
(hd0,1)   second primary partition
(hd0,2)   third primary partition
(hd0,3)   fourth primary partition (usually an extended partition)
(hd0,4)   first logical partition
(hd0,5)   second logical partition
```

In seiner Abhängigkeit von BIOS-Geräten unterscheidet GRUB nicht zwischen IDE-, SATA-, SCSI- und Hardware RAID-Geräten. Alle Festplatten, die vom BIOS oder anderen Controllern erkannt werden, werden der im BIOS voreingestellten Bootreihenfolge entsprechend nummeriert.

Leider ist eine eindeutige Zuordnung zwischen Linux-Gerätenamen und BIOS-Gerätenamen häufig nicht möglich. Es generiert die Zuordnung mithilfe eines Algorithmus und speichert sie in der Datei `device.map`, in der sie bei Bedarf bearbeitet werden kann. Informationen zur Datei `device.map` finden Sie in Abschnitt 8.1.2, „Die Datei "device.map"“ (S. 93).

Ein vollständiger GRUB-Pfad besteht aus einem Gerätenamen, der in Klammern geschrieben wird, und dem Pfad der Datei im Dateisystem auf der angegebenen Partition. Der Pfad beginnt mit einem Schrägstrich. Auf einem System mit einer einzelnen IDE-Festplatte und Linux auf der ersten Partition könnte der bootbare Kernel beispielsweise wie folgt spezifiziert werden:

```
(hd0,0)/boot/vmlinuz
```

Beispiel einer Menüdatei

Das folgende Beispiel zeigt die Struktur einer GRUB-Menüdatei. Diese Beispiel-Installation beinhaltet eine Linux-Bootpartition unter `/dev/sda5`, eine Root-Partition unter `/dev/sda7` und eine Windows-Installation unter `/dev/sda1`.

```
gfxmenu (hd0,4)/boot/message
color white/blue black/light-gray
default 0
timeout 8
```

```
title linux
   root (hd0,4)
   kernel /boot/vmlinuz root=/dev/sda7 vga=791 resume=/dev/sda9
   initrd /boot/initrd

title windows
   rootnoverify (hd0,0)
   chainloader +1

title floppy
   rootnoverify (hd0,0)
   chainloader (fd0)+1

title failsafe
   root (hd0,4)
   kernel /boot/vmlinuz.shipped root=/dev/sda7 ide=nodma \
   apm=off acpi=off vga=normal nosmp maxcpus=0 3 noresume
   initrd /boot/initrd.shipped
```

Der erste Block definiert die Konfiguration des Eröffnungsbildschirms:

gfxmenu (hd0,4)/message
: Das Hintergrundbild `message` befindet sich im Verzeichnis der obersten Ebene der Partition `/dev/sda5`.

color white/blue black/light-gray
: Farbschema: white (Vordergrund), blue (Hintergrund), black (Auswahl) und light gray (Hintergrund der Markierung). Das Farbschema wirkt sich nicht auf den Eröffnungsbildschirm, sondern nur auf das anpassbare GRUB-Menü aus, auf das Sie zugreifen können, wenn Sie den Eröffnungsbildschirm mit Esc beenden.

default 0
: Der erste Menüeintrag `title linux` soll standardmäßig gebootet werden.

timeout 8
: Nach acht Sekunden ohne Benutzereingabe bootet GRUB den Standardeintrag automatisch. Um das automatische Booten zu deaktivieren, löschen Sie die Zeile `timeout`. Wenn Sie `timeout 0` einstellen, bootet GRUB den Standardeintrag sofort.

Im zweiten und größten Block sind die verschiedenen bootbaren Betriebssysteme aufgelistet. Die Abschnitte für die einzelnen Betriebssysteme werden durch `title` eingeleitet.

- Der erste Eintrag (`title linux`) ist für das Booten von SUSE Linux Enterprise Server verantwortlich. Der Kernel (`vmlinuz`) befindet sich in der ersten logischen Partition (die Bootpartition) der ersten Festplatte. Hier werden Kernel-Parameter, z. B. die Root-Partition und der VGA-Modus, angehängt. Die Angabe der root-Partition erfolgt nach der Linux-Namenskonvention (`/dev/sda7/`), da diese Information für den Kernel bestimmt ist und nichts mit GRUB zu tun hat. Die `initrd` befindet sich ebenfalls in der ersten logischen Partition der ersten Festplatte.

- Der zweite Eintrag ist für das Laden von Windows verantwortlich. Windows wird von der ersten Partition der ersten Festplatte aus gebootet (`hd0,0`). Mit `chainloader +1` wird das Auslesen und Ausführen des ersten Sektors der angegebenen Partition gesteuert.

- Der nächste Eintrag dient dazu, das Booten von Diskette zu ermöglichen, ohne dass dazu die BIOS-Einstellungen geändert werden müssten.

- Die Bootoption `failsafe` dient dazu, Linux mit einer bestimmten Auswahl an Kernel-Parametern zu starten, die selbst auf problematischen Systemen ein Hochfahren von Linux ermöglichen.

Die Menüdatei kann jederzeit geändert werden. GRUB verwendet die geänderten Einstellungen anschließend für den nächsten Bootvorgang. Sie können diese Datei mit dem Editor Ihrer Wahl oder mit YaST editieren und dauerhaft speichern. Alternativ können Sie temporäre Änderungen interaktiv über die Bearbeitungsfunktion von GRUB vornehmen. Weitere Informationen hierzu finden Sie unter „Ändern von Menü-Einträgen während des Bootvorgangs“ (S. 92).

Ändern von Menü-Einträgen während des Bootvorgangs

Wählen Sie im grafischen Bootmenü das zu bootende Betriebssystem mit den Pfeiltasten aus. Wenn Sie ein Linux-System wählen, können Sie in der Booteingabeaufforderung zusätzliche Bootparameter eingeben. Um einzelne Menüeinträge direkt zu bearbeiten, drücken Sie die Esc-Taste. Der Eröffnungsbildschirm wird geschlossen und das textbasierte GRUB-Menü aufgerufen. Drücken Sie anschließend die Taste E. Auf diese Weise vorgenommene Änderungen gelten nur für den aktuellen Bootvorgang und können nicht dauerhaft übernommen werden.

WICHTIG: Tastaturbelegung während des Bootvorgangs

Beim Bootvorgang ist nur die amerikanische Tastaturbelegung verfügbar. Eine Abbildung finden Sie in Abbildung „US Keyboard Layout“ (↑*Handbuch für Systemanalyse und Tuning*).

Durch die Möglichkeit, die Menüeinträge zu bearbeiten, kann ein defektes System, das nicht mehr gebootet werden kann, repariert werden, da die fehlerhafte Konfigurationsdatei des Bootloaders mittels der manuellen Eingabe von Parametern umgangen werden kann. Die manuelle Eingabe vom Parametern während des Bootvorgangs ist zudem hilfreich zum Testen neuer Einstellungen, ohne dass diese sich auf das native System auswirken.

Aktivieren Sie den Bearbeitungsmodus und wählen Sie mithilfe der Pfeiltasten den Menüeintrag aus, dessen Konfiguration sie ändern möchten. Um die Konfiguration zu bearbeiten, drücken Sie die Taste E erneut. Auf diese Weise korrigieren Sie falsche Partitions- oder Pfadangaben, bevor sich diese negativ auf den Bootvorgang auswirken. Drücken Sie die Eingabetaste, um den Bearbeitungsmodus zu verlassen und zum Menü zurückzukehren. Drücken Sie anschließend die Taste B, um diesen Eintrag zu booten. Im Hilfetext am unteren Rand werden weitere mögliche Aktionen angezeigt.

Um die geänderten Bootoptionen dauerhaft zu übernehmen und an den Kernel zu übergeben, öffnen Sie die Datei `menu.lst` als Benutzer `root` und hängen Sie die entsprechenden Kernel-Parameter an folgende vorhandene Zeile getrennt durch Leerzeichen an:

```
title linux
   root(hd0,0)
   kernel /vmlinuz root=/dev/sda3 additional parameter
   initrd /initrd
```

GRUB übernimmt den neuen Parameter beim nächsten Booten automatisch. Alternativ können Sie diese Änderung auch mit dem YaST-Bootloader-Modul vornehmen. Hängen Sie die neuen Parameter getrennt durch Leerzeichen an die vorhandene Zeile an.

8.1.2 Die Datei "device.map"

Die Datei `device.map` enthält Zuordnungen zwischen den GRUB- und BIOS-Gerätenamen und den Linux-Gerätenamen. In einem Mischsystem aus IDE- und SCSI-Festplatten muss GRUB anhand eines bestimmten Verfahrens versuchen, die Bootrei-

henfolge zu ermitteln, da die BIOS-Informationen zur Bootreihenfolge für GRUB unter Umständen nicht zugänglich sind. GRUB speichert das Ergebnis dieser Analyse in der Datei `/boot/grub/device.map`. Auf einem System, für das IDE vor SCSI gebootet werden soll, kann die Datei `device.map` beispielsweise wie folgt aussehen:

```
(fd0)   /dev/fd0
(hd0)   /dev/sda
(hd1)   /dev/sdb
```

Da die Reihenfolge von IDE, SCSI und anderen Festplatten abhängig von verschiedenen Faktoren ist und Linux die Zuordnung nicht erkennen kann, besteht die Möglichkeit, die Reihenfolge in der Datei `device.map` manuell festzulegen. Wenn beim Booten Probleme auftreten sollten, prüfen Sie, ob die Reihenfolge in dieser Datei der BIOS-Reihenfolge entspricht, und ändern Sie sie notfalls temporär mithilfe der GRUB-Eingabeaufforderung. Sobald das Linux-System gebootet ist, können Sie die Datei `device.map` mithilfe des YaST-Bootloader-Moduls oder eines Editors Ihrer Wahl dauerhaft bearbeiten.

ANMERKUNG: Maximale Anzahl an Festplatten

Für das Ansprechen einer Festplatte verwendet GRUB BIOS-Dienste. Dies erfolgt über den Software-Interrupt Int13h. Da Int13h auf den Umgang mit maximal acht Festplatten beschränkt ist, kann GRUB nur von diesen durch Int13h verwalteten Platten booten, selbst wenn mehr Festplatten vorhanden sind (was häufig auf Mehrwegesystemen der Fall ist). Die Datei `device.map`, die bei der Installation erstellt wurde, enthält daher nur eine Höchstanzahl von acht Festplatten, die von Int13h verwaltet werden.

Installieren Sie nach der manuellen Bearbeitung von `device.map` GRUB über den folgenden Befehl erneut. Dieser Befehl führt dazu, dass die Datei `device.map` neu geladen wird und die in `grub.conf` aufgelisteten Befehle ausgeführt werden:

```
grub --batch < /etc/grub.conf
```

8.1.3 Die Datei "/etc/grub.conf"

Nach `menu.lst` und `device.map` ist `/etc/grub.conf` die dritte wichtige Konfigurationsdatei von GRUB. Diese Datei enthält die Befehle, Parameter und Optionen, die die GRUB-Shell für das ordnungsgemäße Installieren des Bootloaders benötigt.

```
setup --stage2=/boot/grub/stage2 --force-lba (hd0,1) (hd0,1)
   quit
```

Dieses Kommando weist GRUB an, den Bootloader automatisch auf die zweite Partition der ersten Festplatte (hd0,1) zu installieren und dabei die Boot-Images zu verwenden, die sich auf derselben Partition befinden. Der Parameter `--stage2=/boot/grub/stage2` ist erforderlich, um das Image `stage2` von einem eingehängten Dateisystem zu installieren. Einige BIOS haben eine fehlerhafte Implementierung für LBA-Unterstützung. Mit `--force-lba` können Sie diese ignorieren.

8.1.4 Festlegen eines Bootpassworts

Schon vor dem Booten des Betriebssystems ermöglicht GRUB den Zugriff auf Dateisysteme. Dies bedeutet, dass Benutzer ohne root-Berechtigungen auf Dateien des Linux-Systems zugreifen können, auf die sie nach dem Booten keinen Zugriff haben. Um diese Zugriffe oder das Booten bestimmter Betriebssysteme zu verhindern, können Sie ein Bootpasswort festlegen.

WICHTIG: Bootpasswort und Eröffnungsbildschirm

Wenn Sie für GRUB ein Bootpasswort verwenden, wird der übliche Eröffnungsbildschirm nicht angezeigt.

Legen Sie als Benutzer `root` das Bootpasswort wie folgt fest:

1. Verschlüsseln Sie an der root-Eingabeaufforderung das Passwort mithilfe von grub-md5-crypt:

   ```
   # grub-md5-crypt
   Password: ****
   Retype password: ****
   Encrypted: $1$lS2dv/$JOYcdxIn7CJk9xShzzJVw/
   ```

2. Fügen Sie die verschlüsselte Zeichenkette in den globalen Abschnitt der Datei `menu.lst` ein:

   ```
   gfxmenu (hd0,4)/message
   color white/blue black/light-gray
   default 0
   timeout 8
   password --md5 $1$lS2dv/$JOYcdxIn7CJk9xShzzJVw/
   ```

Jetzt können GRUB-Befehle in der Booteingabeaufforderung nur ausgeführt werden, wenn die Taste P gedrückt und das Passwort eingegeben wurde. Benutzer können jedoch über das Bootmenü weiterhin alle Betriebssysteme booten.

3 Um zu verhindern, dass ein oder mehrere Betriebssysteme über das Bootmenü gebootet werden, fügen Sie den Eintrag `lock` zu allen Abschnitten in `menu.lst` hinzu, die ohne Eingabe eines Passworts nicht gebootet werden sollen. Beispiel:

```
title linux
   kernel (hd0,4)/vmlinuz root=/dev/sda7 vga=791
   initrd (hd0,4)/initrd
   lock
```

Nach dem Neubooten des Systems und der Auswahl des Linux-Eintrags im Bootmenü erscheint zunächst folgende Fehlermeldung:

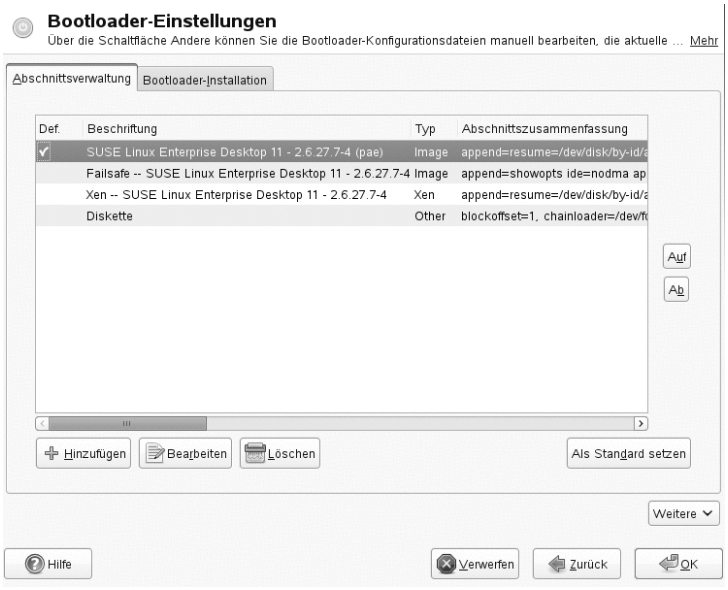
```
Error 32: Must be authenticated
```

Drücken Sie die Eingabetaste, um das Menü zu öffnen. Drücken Sie anschließend die Taste P, um die Eingabeaufforderung für das Passwort zu öffnen. Wenn Sie das Passwort eingegeben und die Eingabetaste gedrückt haben, sollte das ausgewählte Betriebssystem (in diesem Fall Linux) gebootet werden.

8.2 Konfigurieren des Bootloaders mit YaST

Mit dem YaST-Modul ist die Konfiguration des Bootloaders auf Ihrem SUSE Linux Enterprise Server-System am einfachsten. Wählen Sie im YaST-Kontrollzentrum *System* > *Bootloader*. Wie in Abbildung 8.1, „Bootloader-Einstellungen“ (S. 97) zeigt dies die aktuelle Bootloader-Konfiguration des Systems und ermöglicht Ihnen, Änderungen vorzunehmen.

Abbildung 8.1 *Bootloader-Einstellungen*



Auf dem Karteireiter *Abschnittsverwaltung* können Sie die Bootloader-Abschnitte für die einzelnen Betriebssysteme bearbeiten, ändern und löschen. Klicken Sie auf *Hinzufügen*, um eine Option hinzuzufügen. Wenn Sie den Wert einer bestehenden Option ändern möchten, wählen Sie ihn mit der Maus aus und klicken Sie auf *Bearbeiten*. Um ein vorhandenes Schema zu löschen, wählen Sie das Schema aus und klicken Sie auf *Löschen*. Wenn Sie nicht mit den Bootloader-Optionen vertraut sind, lesen Sie zunächst Abschnitt 8.1, „Booten mit GRUB“ (S. 86).

Verwenden Sie die Karteireiter *Bootloader-Installation*, um die Einstellungen in Bezug auf Typ, Speicherort und erweiterte Bootloader-Einstellungen anzuzeigen und zu ändern.

Erweiterte Konfigurationsoptionen erhalten Sie im Dropdown-Menü der Option *Andere*. Über den integrierten Editor können Sie die GRUB-Konfigurationsdateien ändern (Einzelheiten finden Sie unter Abschnitt 8.1, „Booten mit GRUB“ (S. 86)). Sie können die vorhandene Konfiguration auch löschen und eine *neue Konfiguration ohne Vorschlag erstellen* oder sich von YaST *eine neue Konfiguration vorschlagen lassen*. Sie können die Konfiguration auch auf die Festplatte schreiben und sie von der Festplatte wieder einlesen. Zur Wiederherstellung des ursprünglichen, während der Installation gespeicherten MBR (Master Boot Record) wählen Sie *MBR von Festplatte wiederherstellen* aus.

8.2.1 Anpassen des Standard-Boot-Eintrags

Um das System zu ändern, das standardmäßig gebootet wird, gehen Sie wie folgt vor:

Prozedur 8.1 *Standardsystem einrichten*

1. Öffnen Sie die Karteireiter *Abschnittsverwaltung*.
2. Wählen Sie den gewünschten Eintrag in der Liste aus.
3. Klicken Sie auf *Als Standard festlegen*.
4. Klicken Sie auf *Verlassen*, um die Änderungen zu aktivieren.

8.2.2 Speicherort des Bootloaders ändern

Um den Speicherort des Bootloaders zu ändern, gehen Sie wie folgt vor:

Prozedur 8.2 *Speicherort des Bootloaders ändern*

1. Wählen Sie den Karteireiter *Bootloader-Installation* und anschließend eine der folgenden Optionen für *Speicherort des Bootloaders*:

   Booten von der Bootpartition
   : Der Bootsektor der Partition `/boot`.

   Booten von der erweiterten Partition
   : Der Bootloader wird in den Container der erweiterten Partition installiert.

   Booten vom Master Boot Record
   : Der Bootloader wird in den MBR des ersten Laufwerks installiert (entsprechend der im BIOS voreingestellten Bootreihenfolge).

   Booten von der root-Partition
   : Der Bootloader wird in den Bootsektor der Partition `/` installiert.

   Benutzerdefinierte Bootpartition
   : Mit dieser Option können Sie den Speicherort des Bootloaders manuell angeben.

2 Klicken Sie zum Anwenden der Einstellungen auf *Verlassen*.

8.2.3 Ändern des Bootloader-Zeitlimits

Der Bootloader bootet das Standardsystem nicht sofort. Während des Zeitlimits können Sie das zu bootende System auswählen oder einige Kernel-Parameter schreiben. Gehen Sie wie folgt vor, um das Zeitlimit des Bootloaders festzulegen:

Prozedur 8.3 *Ändern des Bootloader-Zeitlimits*

1 Öffnen Sie die Karteireiter *Bootloader-Installation*.

2 Klicken Sie auf *Bootloader-Optionen*.

3 Ändern Sie den Wert für *Zeitüberschreitung in Sekunden*, indem Sie einen neuen Wert eingeben, mit der Maus auf den entsprechenden Pfeil klicken oder die Pfeiltasten der Tastatur verwenden.

4 Klicken Sie auf *OK*.

5 Klicken Sie auf *Verlassen*, um die Änderungen zu speichern.

8.2.4 Festlegen eines Bootpassworts

Mit diesem YaST-Modul können Sie zum Schutz des Bootvorgangs auch ein Passwort einrichten. Damit wird ein zusätzlicher Grad an Sicherheit geboten.

Prozedur 8.4 *Festlegen eines Bootloader-Passworts*

1 Öffnen Sie die Karteireiter *Bootloader-Installation*.

2 Klicken Sie auf *Bootloader-Optionen*.

3 Geben Sie in *Passwort für die Menüschnittstelle* Ihr Passwort an.

4 Klicken Sie auf *OK*.

5 Klicken Sie auf *Verlassen*, um die Änderungen zu speichern.

8.2.5 Anpassen der Festplattenreihenfolge

Wenn Ihr Computer mehrere Festplatten hat, können Sie die Bootsequenz der Festplatten so festlegen, dass sie dem BIOS-Setup des Computers entsprechen (siehe Abschnitt 8.1.2, „Die Datei "device.map"“ (S. 93)). Gehen Sie hierfür wie folgt vor:

Prozedur 8.5 *Festlegen der Festplattenreihenfolge*

1. Öffnen Sie die Karteireiter *Bootloader-Installation*.
2. Klicken Sie auf *Details zur Bootloader-Installation*.
3. Ändern Sie bei mehreren aufgeführten Festplatten deren Reihenfolge mit einem Klick auf *Auf* oder *Ab*.
4. Klicken Sie zum Speichern der Änderungen auf *OK*.
5. Klicken Sie auf *Verlassen*, um die Änderungen zu speichern.

8.2.6 Konfigurieren der erweiterten Optionen

Erweiterte Boot-Optionen lassen sich über *Bootloader-Installation* > *Bootloader-Optionen* konfigurieren. Normalerweise sollte es nicht erforderlich sein, die Standardeinstellungen zu ändern.

Aktives Flag in Partitionstabelle für Bootpartition festlegen
: Aktiviert die Partition, die den Bootloader enthält. Einige ältere Betriebssysteme, z. B. Windows 98, können nur von einer aktiven Partition booten.

Flag für Durchführung der Fehlersuche
: Stellt GRUB in den Fehlersuchmodus um, in dem Meldungen über die Plattenaktivität angezeigt werden.

Generischen Bootcode in MBR schreiben
: Ersetzt den aktuellen MBR durch generischen, Betriebssystem-unabhängigen Code.

Menü beim Booten ausblenden
: Blendet das Bootmenü aus und bootet den Standardeintrag.

Trusted GRUB verwenden
: Startet Trusted GRUB, das verbürgte Computerfunktionen unterstützt.

Datei für grafisches Menü
: Pfad zur Grafikdatei, die bei der Anzeige des Boot-Bildschirms verwendet wird.

Parameter der seriellen Verbindung
: Wenn Ihr Computer über eine serielle Konsole gesteuert wird, können Sie angeben, welcher COM-Port in welcher Geschwindigkeit verwendet werden soll. Stellen Sie auch *Terminaldefinition* auf "Seriell" ein. Einzelheiten finden Sie unter `info grub` oder `http://www.gnu.org/software/grub/manual/grub.html`.

Terminaldefinition
: Wenn Sie über eine serielle Konsole booten, geben Sie hier "Seriell" ein. (Andernfalls lassen Sie das Feld leer.) In diesem Fall müssen Sie auch *Parameter der seriellen Verbindung* eingeben.

8.2.7 Ändern des Bootloader-Typs

Legen Sie den Bootloader-Typ unter *Bootloader-Installation* fest. In SUSE Linux Enterprise Server wird standardmäßig der Bootloader GRUB verwendet. Gehen Sie wie folgt vor, wenn Sie LILO verwenden möchten:

Prozedur 8.6 *Ändern des Bootloader-Typs*

1. Wählen Sie die Karteireiter *Bootloader-Installation*.
2. Wählen Sie unter *Bootloader* die Option *LILO*.
3. Wählen Sie in dem sich öffnenden Dialogfeld folgende Aktionen aus:

   Neue Konfiguration vorschlagen
   : Lässt YaST eine neue Konfiguration erstellen.

Aktuelle Konfiguration konvertieren
: Lässt YaST die aktuelle Konfiguration konvertieren. Es ist möglich, dass beim Konvertieren der Konfiguration einige Einstellungen verloren gehen.

Neue Konfiguration ohne Vorschlag erstellen
: Erstellt eine benutzerdefinierte Konfiguration. Diese Aktion ist während der Installation von SUSE Linux Enterprise Server nicht verfügbar.

Auf Festplatte gespeicherte Konfiguration einlesen
: Lädt Ihre eigene Datei `/etc/lilo.conf`. Diese Aktion ist während der Installation von SUSE Linux Enterprise Server nicht verfügbar.

4 Klicken Sie zum Speichern der Änderungen auf *OK*

5 Klicken Sie im Hauptdialogfeld auf *Verlassen*, um die Änderungen zu übernehmen.

Während der Konvertierung wird die alte GRUB-Konfiguration gespeichert. Wenn Sie sie verwenden möchten, ändern Sie einfach den Bootloader-Typ zurück in GRUB und wählen Sie *Vor der Konvertierung gespeicherte Konfiguration wiederherstellen*. Diese Aktion ist nur auf einem installierten System verfügbar.

ANMERKUNG: Benutzerdefinierter Bootloader

Wenn Sie einen anderen Bootloader als GRUB oder LILO verwenden möchten, wählen Sie *Keinen Bootloader installieren*. Lesen Sie die Dokumentation Ihres Bootloaders sorgfältig durch, bevor Sie diese Option auswählen.

8.3 Deinstallieren des Linux-Bootloaders

Mit YaST können Sie den Linux-Bootloader deinstallieren und den Zustand des MBR vor der Installation wiederherstellen. YaST erstellt während der Installation automatisch ein Backup der ursprünglichen MBR-Version und stellt sie bei Bedarf wieder her.

Um GRUB zu deinstallieren, starten Sie das YaST-Bootloader-Modul (*System* > *Bootloader*). Wählen Sie *Andere* > *MBR von Festplatte wiederherstellen* aus und bestätigen Sie mit *Yes, Rewrite*.

8.4 Erstellen von Boot-CDs

Wenn beim Booten Ihres Systems unter Verwendung eines Bootmanagers Probleme auftreten oder wenn der Bootmanager auf dem MBR Ihrer Festplatte oder einer Diskette nicht installiert werden kann, ist es auch möglich, eine bootfähige CD mit all den für Linux erforderlichen Startdateien zu erstellen. Hierfür muss ein CD-Brenner in Ihrem System installiert sein.

Für die Erstellung einer bootfähigen CD-ROM mit GRUB ist lediglich eine spezielle Form von *stage2* mit Namen `stage2_eltorito` erforderlich sowie optional eine benutzerdefinierte Datei `menu.lst`. Die klassischen Dateien `stage1` und `stage2` sind nicht erforderlich.

Prozedur 8.7 *Erstellen von Boot-CDs*

1. Wechseln Sie in ein Verzeichnis, in dem das ISO-Image erstellt werden soll, beispielsweise: `cd /tmp`

2. Erstellen Sie ein Unterverzeichnis für GRUB und wechseln Sie in das neu erstellte `iso`-Verzeichnis:

   ```
   mkdir -p iso/boot/grub && cd iso
   ```

3. Kopieren Sie den Kernel, die Dateien `stage2_eltorito`, `initrd`, `menu.lst` und `/message` nach `iso/boot/`:

   ```
   cp /boot/vmlinuz boot/
   cp /boot/initrd boot/
   cp /boot/message boot/
   cp /usr/lib/grub/stage2_eltorito boot/grub
   cp /boot/grub/menu.lst boot/grub
   ```

4. Passen Sie die Pfadeinträge in `boot/grub/menu.lst` so an, dass sie auf ein CD-ROM-Laufwerk verweisen. Ersetzen Sie hierfür in den Pfadnamen den Gerätenamen der Festplatten, die im Format `(hd`*`x,y`*`)` aufgeführt sind, durch den Gerätenamen des CD-ROM-Laufwerks, das mit `(cd)` angegeben wird. Sie müssen unter Umständen auch die Pfade zur Meldungsdatei, zum Kernel und zur initrd-Datei anpassen, sodass sie auf `/boot/message`, `/boot/vmlinuz` bzw. `/boot/initrd` verweisen. Nachdem Sie die Anpassungen durchgeführt haben, sollte `menu.lst` wie im folgenden Beispiel aussehen:

```
timeout 8
default 0
gfxmenu (cd)/boot/message

title Linux
   root (cd)
   kernel /boot/vmlinuz root=/dev/sda5 vga=794 resume=/dev/sda1 \
   splash=verbose showopts
   initrd /boot/initrd
```

Verwenden Sie `splash=silent` anstelle von `splash=verbose`, um zu vermeiden, dass beim Bootvorgang Bootmeldungen angezeigt werden.

5 Erstellen Sie das ISO-Image mit dem folgenden Befehl:

```
genisoimage -R -b boot/grub/stage2_eltorito -no-emul-boot \
-boot-load-size 4 -boot-info-table -iso-level 2 -input-charset utf-8 \
-o grub.iso /tmp/iso
```

6 Schreiben Sie die so erstellte Datei namens `grub.iso` unter Verwendung Ihres bevorzugten Dienstprogramms auf eine CD. Brennen Sie das ISO-Image nicht als Datendatei, sondern verwenden Sie die Option zum Brennen eines CD-Images, die in Ihrem Dienstprogramm angeboten wird.

8.5 Der grafische SUSE-Bildschirm

Der grafische SUSE-Bildschirm wird auf der ersten Konsole angezeigt, wenn die Option `vga=<Wert >` als Kernel-Parameter verwendet wird. Bei der Installation mit YaST wird diese Option automatisch in Abhängigkeit von der gewählten Auflösung und der verwendeten Grafikkarte aktiviert. Sie haben bei Bedarf drei Möglichkeiten, den SUSE-Bildschirm zu deaktivieren:

Den SUSE-Bildschirm bei Bedarf deaktivieren
: Geben Sie den Befehl `echo 0 >/proc/splash` in der Kommandozeile ein, um den grafischen Bildschirm zu deaktivieren. Um ihn wieder zu aktivieren, geben Sie den Befehl `echo 1 >/proc/splash` ein.

Den SUSE-Bildschirm standardmäßig deaktivieren
: Fügen Sie der Bootloader-Konfiguration den Kernel-Parameter `splash=0` hinzu. Weitere Informationen hierzu finden Sie in Kapitel 8, *Der Bootloader GRUB*

(S. 85). Wenn Sie jedoch den Textmodus wie in früheren Versionen bevorzugen, legen Sie Folgendes fest: `vga=normal`.

Den SUSE-Bildschirm vollständig deaktivieren
: Kompilieren Sie einen neuen Kernel und deaktivieren Sie die Option zum *Verwenden des Eröffnungsbildschirms anstelle des Bootlogos im Menü Framebuffer-Unterstützung*.

TIPP

Wenn Sie im Kernel die Framebuffer-Unterstützung deaktiviert haben, ist der Eröffnungsbildschirm automatisch auch deaktiviert. Wenn Sie einen eigenen Kernel kompilieren, kann SUSE dafür keinen Support garantieren.

8.6 Fehlersuche

In diesem Abschnitt werden einige der Probleme, die beim Booten mit GRUB auftreten können, sowie deren Lösungen behandelt. Einige der Probleme werden in den Artikeln in der Support-Datenbank unter `http://support.novell.com/` beschrieben. Verwenden Sie das Dialogfeld "Suche", um nach Schlüsselwörtern wie *GRUB*, *boot* und *Bootloader* zu suchen.

GRUB und XFS
: XFS lässt im Partitions-Bootblock keinen Platz für `stage1`. Sie dürfen also als Speicherort des Bootloaders keinesfalls eine XFS-Partition angeben. Um dieses Problem zu beheben, erstellen Sie eine separate Bootpartition, die nicht mit XFS formatiert ist.

GRUB meldet GRUB Geom Error
: GRUB überprüft die Geometrie der angeschlossenen Festplatten beim Booten des Systems. In seltenen Fällen macht das BIOS hier inkonsistente Angaben, sodass GRUB einen "GRUB Geom Error" meldet. Aktualisieren Sie in diesem Fall das BIOS.

  GRUB gibt diese Fehlermeldung auch aus, wenn Linux auf einer zusätzlichen Festplatte im System installiert wurde, diese aber nicht im BIOS registriert ist. Der erste Teil des Bootloaders *stage1* wird korrekt gefunden und geladen, die zweite

Stufe *stage2* wird jedoch nicht gefunden. Dieses Problem können Sie umgehen, indem Sie die neue Festplatte unverzüglich im BIOS registrieren.

System mit mehreren Festplatten startet nicht
: Möglicherweise wurde die Bootsequenz der Festplatten während der Installation von YaST falsch ermittelt. So erkennt GRUB die IDE-Festplatte unter Umständen als `hd0` und die SCSI-Festplatte als `hd1`, obwohl im BIOS die umgekehrte Reihenfolge (SCSI *vor* IDE) angegeben ist.

  Korrigieren Sie in solchen Fällen mithilfe der GRUB-Kommandozeile beim Booten die verwendeten Festplatten. Bearbeiten Sie im gebooteten System die Datei `device.map`, um die neue Zuordnung dauerhaft festzulegen. Überprüfen Sie anschließend die GRUB -Gerätenamen in den Dateien `/boot/grub/menu.lst` und `/boot/grub/device.map` und installieren Sie den Bootloader mit dem folgenden Befehl neu:

```
grub --batch < /etc/grub.conf
```

Windows von der zweiten Festplatte booten
: Einige Betriebssysteme, z. B. Windows, können nur von der ersten Festplatte gebootet werden. Wenn ein solches Betriebssystem auf einer anderen als der ersten Festplatte installiert ist, können Sie für den entsprechenden Menüeintrag einen logischen Tausch veranlassen.

```
...
title windows
   map (hd0) (hd1)
   map (hd1) (hd0)
   chainloader(hd1,0)+1
...
```

  In diesem Beispiel soll Windows von der zweiten Festplatte gestartet werden. Zu diesem Zweck wird die logische Reihenfolge der Festplatten mit `map` getauscht. Die Logik innerhalb der GRUB-Menüdatei ändert sich dadurch jedoch nicht. Daher müssen Sie bei `chainloader` nach wie vor die zweite Festplatte angeben.

8.7 Weiterführende Informationen

Umfassende Informationen zu GRUB finden Sie auf der Webseite unter `http://www.gnu.org/software/grub/`. Ausführliche Informationen finden Sie auch auf der Infoseite für den Befehl `grub`. Weitere Informationen zu bestimmten Themen

erhalten Sie auch, wenn Sie "GRUB" in der Suchfunktion für technische Informationen unter `http://www.novell.com/support` als Suchwort eingeben.

9 Spezielle Systemfunktionen

In diesem Kapitel erhalten Sie zunächst Informationen zu den verschiedenen Softwarepaketen, zu den Virtuellen Konsolen und zur Tastaturbelegung. Hier finden Sie Hinweise zu Software-Komponenten, wie `bash`, `cron` und `logrotate`, da diese im Laufe der letzten Veröffentlichungszyklen geändert oder verbessert wurden. Selbst wenn sie nur klein sind oder als nicht besonders wichtig eingestuft werden, können die Benutzer ihr Standardverhalten ändern, da diese Komponenten häufig eng mit dem System verbunden sind. Das Kapitel endet mit einem Abschnitt mit sprach- und landesspezifischen Einstellungen (I18N und L10N).

9.1 Informationen zu speziellen Softwarepaketen

Die Programme `bash`, `cron`, `logrotate`, `locate`, `ulimit` und `free` spielen für Systemadministratoren und viele Benutzer eine wichtige Rolle. man-Seiten und info-Seiten sind hilfreiche Informationsquellen zu Befehlen, sind jedoch nicht immer verfügbar. GNU Emacs ist ein beliebter konfigurierbarer Texteditor.

9.1.1 Das Paket bash und /etc/profile

Bash ist die Standard-System-Shell. Wenn sie als Anmelde-Shell verwendet wird, werden mehrere Initialisierungsdateien gelesen. Bash verarbeitet die entsprechenden Informationen in der Reihenfolge dieser Liste:

1. `/etc/profile`
2. `~/.profile`
3. `/etc/bash.bashrc`
4. `~/.bashrc`

Nehmen Sie benutzerdefinierte Einstellungen in `~/.profile` oder `~/.bashrc` vor. Um die richtige Verarbeitung der Dateien zu gewährleisten, müssen die Grundeinstellungen aus `/etc/skel/.profile` oder `/etc/skel/.bashrc` in das Home-Verzeichnis des Benutzers kopiert werden. Es empfiehlt sich, die Einstellungen aus `/etc/skel` nach einer Aktualisierung zu kopieren. Führen Sie die folgenden Shell-Befehle aus, um den Verlust persönlicher Einstellungen zu vermeiden:

```
mv ~/.bashrc ~/.bashrc.old
cp /etc/skel/.bashrc ~/.bashrc
mv ~/.profile ~/.profile.old
cp /etc/skel/.profile ~/.profile
```

Kopieren Sie anschließend die persönlichen Einstellungen erneut aus den `*.old`-Dateien.

9.1.2 Das cron-Paket

Wenn Sie Kommandos regelmäßig und automatisch zu bestimmten Zeiten im Hintergrund ausführen möchten, verwenden Sie dazu am besten das Tool cron. cron wird durch speziell formatierte Zeittabellen gesteuert. Einige sind bereits im Lieferumfang des Systems enthalten, bei Bedarf können Benutzer jedoch auch eigene Tabellen erstellen.

Die cron-Tabellen befinden sich im Verzeichnis `/var/spool/cron/tabs`. `/etc/crontab` dient als systemübergreifende cron-Tabelle. Geben Sie den Benutzernamen zur Ausführung des Befehls unmittelbar nach der Zeittabelle und noch vor dem Befehl ein. In Beispiel 9.1, „Eintrag in /etc/crontab“ (S. 110), wird `root` eingegeben. Die paketspezifischen Tabellen in `/etc/cron.d` weisen alle dasselbe Format auf. Informationen hierzu finden Sie auf der Manualpage zu `cron` (`man cron`).

Beispiel 9.1 *Eintrag in /etc/crontab*

```
1-59/5 * * * *   root   test -x /usr/sbin/atrun && /usr/sbin/atrun
```

Sie können /etc/crontab nicht bearbeiten, indem Sie den Befehl crontab -e bearbeiten. Die Datei muss direkt in einem Editor geladen, geändert und dann gespeichert werden.

Einige Pakte installieren Shell-Skripten in die Verzeichnisse /etc/cron.hourly, /etc/cron.daily, /etc/cron.weekly und /etc/cron.monthly, deren Ausführung durch /usr/lib/cron/run-crons gesteuert wird. /usr/lib/cron/run-crons wird alle 15 Minuten von der Haupttabelle (/etc/crontab) ausgeführt. Hiermit wird gewährleistet, dass vernachlässigte Prozesse zum richtigen Zeitpunkt ausgeführt werden können.

Um die Skripten hourly, dailyoder andere Skripten für regelmäßige Wartungsarbeiten zu benutzerdefinierten Zeiten auszuführen, entfernen Sie regelmäßig die Zeitstempeldateien mit/etc/crontab-Einträgen (siehe Beispiel 9.2, „/etc/crontab: Entfernen der Zeitstempeldateien“ (S. 111) - u. a. wird hourly vor jeder vollen Stunde und daily einmal täglich um 2:14 Uhr entfernt).

Beispiel 9.2 *„/etc/crontab: Entfernen der Zeitstempeldateien“*

```
59 *  * * *     root  rm -f /var/spool/cron/lastrun/cron.hourly
14 2  * * *     root  rm -f /var/spool/cron/lastrun/cron.daily
29 2  * * 6     root  rm -f /var/spool/cron/lastrun/cron.weekly
44 2  1 * *     root  rm -f /var/spool/cron/lastrun/cron.monthly
```

Stellen Sie DAILY_TIME in /etc/sysconfig/cron alternativ auf die Zeit ein, zu der cron.daily gestartet werden soll. Mit MAX_NOT_RUN stellen Sie sicher, dass die täglichen Aufträge auch dann ausgeführt werden, wenn der Computer zur angegebenen DAILY_TIME und auch eine längere Zeit danach nicht eingeschaltet ist. Die maximale Einstellung von MAX_NOT_RUN sind 14 Tage.

Die täglichen Systemwartungsaufträge werden zum Zwecke der Übersichtlichkeit auf mehrere Skripts verteilt. Sie sind im Paket aaa_base enthalten. /etc/cron.daily enthält beispielsweise die Komponenten suse.de-backup-rpmdb, suse.de-clean-tmp oder suse.de-cron-local.

9.1.3 Protokolldateien: Paket logrotate

Mehrere Systemdienste (*Daemons*) zeichnen zusammen mit dem Kernel selbst regelmäßig den Systemstatus und spezielle Ereignisse in Protokolldateien auf. Auf diese

Weise kann der Administrator den Status des Systems zu einem bestimmten Zeitpunkt regelmäßig überprüfen, Fehler oder Fehlfunktionen erkennen und die Fehler mit Präzision beheben. Die Protokolldateien werden in der Regel, wie von FHS angegeben, unter `/var/log` gespeichert und werden täglich umfangreicher. Mit dem Paket `logrotate` kann der Umfang der Dateien gesteuert werden.

Konfigurieren Sie Logrotate mit der Datei `/etc/logrotate.conf`. Die Dateien, die zusätzlich gelesen werden sollen, werden insbesondere durch die `include`-Spezifikation konfiguriert. Programme, die Protokolldateien erstellen, installieren einzelne Konfigurationsdateien in `/etc/logrotate.d`. Solche Dateien sind beispielsweise im Lieferumfang der Pakete `apache2` (`/etc/logrotate.d/apache2`) und `syslogd` (`/etc/logrotate.d/syslog`) enthalten.

Beispiel 9.3 *Beispiel für /etc/logrotate.conf*

```
# see "man logrotate" for details
# rotate log files weekly
weekly

# keep 4 weeks worth of backlogs
rotate 4

# create new (empty) log files after rotating old ones
create

# uncomment this if you want your log files compressed
#compress

# RPM packages drop log rotation information into this directory
include /etc/logrotate.d

# no packages own lastlog or wtmp - we'll rotate them here
#/var/log/wtmp {
#    monthly
#    create 0664 root utmp
#    rotate 1
#}

# system-specific logs may be also be configured here.
```

logrotate wird über cron gesteuert und täglich durch `/etc/cron.daily/logrotate` aufgerufen.

WICHTIG

Mit der Option `create` werden alle vom Administrator in `/etc/permissions*` vorgenommenen Einstellungen gelesen. Stellen Sie sicher, dass durch persönliche Änderungen keine Konflikte auftreten.

9.1.4 Der Befehl "locate"

locate, ein Befehl zum schnellen Suchen von Dateien ist nicht im Standardumfang der installierten Software enthalten. Wenn Sie möchten, installieren Sie das Paket `findutils-locate`. Der Prozess updatedb wird jeden Abend etwa 15 Minuten nach dem Booten des Systems gestartet.

9.1.5 Der Befehl "ulimit"

Mit dem Befehl `ulimit` (*user limits*) können Grenzwerte für die Verwendung der Systemressourcen festgelegt und angezeigt werden. `ulimit` ist insbesondere für die Begrenzung des für Anwendungen verfügbaren Speichers hilfreich. Hiermit kann verhindert werden, dass eine Anwendung zu viel Speicher belegt, wodurch es zu einem Stillstand des Systems kommen kann.

`ulimit` kann mit verschiedenen Optionen verwendet werden. Verwenden Sie zum Begrenzen der Speicherauslastung die in Tabelle 9.1, „`ulimit`: Einstellen von Ressourcen für Benutzer“ (S. 113) aufgeführten Optionen.

Tabelle 9.1 *ulimit: Einstellen von Ressourcen für Benutzer*

`-m`	Die maximale nicht auslagerbare festgelegte Größe
`-v`	Die maximale Größe des virtuellen Arbeitsspeichers, der der Shell zur Verfügung steht
`-s`	Die maximale Größe des Stapels
`-c`	Die maximale Größe der erstellten Kerndateien

`-a`	Alle aktuellen Grenzwerte werden gemeldet

In `/etc/profile` können Sie systemweite Einträge vornehmen. Aktivieren Sie hier die Erstellung der Core-Dateien, die Programmierer für die *Fehlersuche* benötigen. Ein normaler Benutzer kann die in `/etc/profile` vom Systemadministrator festgelegten Werte nicht erhöhen, er kann jedoch spezielle Einträge in `~/.bashrc` vornehmen.

Beispiel 9.4 *ulimit: Einstellungen in ~/.bashrc*

```
# Limits maximum resident set size (physical memory):
ulimit -m 98304

# Limits of virtual memory:
ulimit -v 98304
```

Die Speicherangaben müssen in KB erfolgen. Weitere Informationen erhalten Sie mit `man bash`.

WICHTIG

ulimit-Direktiven werden nicht von allen Shells unterstützt. PAM (beispielsweise `pam_limits`) bietet umfassende Anpassungsmöglichkeiten, wenn Sie Einstellungen für diese Beschränkungen vornehmen müssen.

9.1.6 Der Befehl "free"

Der Befehl `free` ist leicht irreführend, wenn Sie herausfinden möchten, wie viel Arbeitsspeicher zurzeit verwendet wird. Die entsprechenden Informationen finden Sie in `/proc/meminfo`. Heute müssen sich Benutzer, die ein modernes Betriebssystem wie Linux verwenden, in der Regel kaum Gedanken über den Arbeitsspeicher machen. Das Konzept des *verfügbaren Arbeitsspeichers* geht auf Zeiten vor der einheitlichen Speicherverwaltung zurück. Bei Linux gilt der Grundsatz *freier Arbeitsspeicher ist schlechter Arbeitsspeicher.* Daher wurde bei Linux immer darauf geachtet, die Caches auszugleichen, ohne freien oder nicht verwendeten Arbeitsspeicher zuzulassen.

Der Kernel verfügt nicht direkt über Anwendungs- oder Benutzerdaten. Stattdessen verwaltet er Anwendungen und Benutzerdaten in einem *Seiten-Cache*. Falls nicht mehr genügend Arbeitsspeicher vorhanden ist, werden Teile auf der Swap-Partition oder in

Dateien gespeichert, von wo aus sie mithilfe des Befehls `mmap` abgerufen werden können. (siehe `man mmap`).

Der Kernel enthält zusätzlich andere Caches, wie beispielsweise den *slab-Cache*, in dem die für den Netzwerkzugriff verwendeten Caches gespeichert werden. Dies erklärt die Unterschiede zwischen den Zählern in `/proc/meminfo`. Die meisten, jedoch nicht alle dieser Zähler können über `/proc/slabinfo` aufgerufen werden.

9.1.7 man-Seiten und Info-Seiten

Für einige GNU-Anwendungen (wie beispielsweise tar) sind keine man-Seiten mehr vorhanden. Verwenden Sie für diese Befehle die Option `--help`, um eine kurze Übersicht über die info-Seiten zu erhalten, in der Sie detailliertere Anweisungen erhalten. info befindet sich im Hypertextsystem von GNU. Eine Einführung in dieses System erhalten Sie, wenn Sie `infoinfo` eingeben. Info-Seiten können mit Emacs angezeigt werden, wenn Sie `emacs -f info` eingeben oder mit `info` direkt in einer Konsole angezeigt werden. Sie können auch tkinfo, xinfo oder das Hilfesystem von zum Anzeigen von info-Seiten verwenden.

9.1.8 Auswählen von man-Seiten mit dem Kommando man

Mit `man` *`man-page`* zeigen Sie normalerweise eine man-Seite direkt zum Lesen an. Wenn eine man-Seite mit demselben Namen in verschiedenen Abschnitten vorhanden ist, fordert `man` den Benutzer auf, den Abschnitt anzugeben, aus dem die Seite angezeigt werden soll.

Wenn Sie zum vorherigen Verhalten zurückkehren möchten, setzen Sie `MAN_POSIXLY_CORRECT=1` in einer Shell-Initialisierungsdatei wie `~/.bashrc`.

9.1.9 Einstellungen für GNU Emacs

GNU Emacs ist eine komplexe Arbeitsumgebung. In den folgenden Abschnitten werden die beim Starten von GNU Emacs verarbeiteten Dateien beschrieben. Weitere Informa-

tionen hierzu erhalten Sie online unter `http://www.gnu.org/software/emacs/`.

Beim Starten liest Emacs mehrere Dateien, in denen die Einstellungen für den Benutzer, den Systemadministrator und den Distributor zur Anpassung oder Vorkonfiguration enthalten sind. Die Initialisierungsdatei `~/.emacs` ist in den Home-Verzeichnissen der einzelnen Benutzer von `/etc/skel` installiert. `.emacs` wiederum liest die Datei `/etc/skel/.gnu-emacs`. Zum Anpassen des Programms kopieren Sie `.gnu-emacs` in das Home-Verzeichnis (mit `cp /etc/skel/.gnu-emacs ~/.gnu-emacs`) und nehmen Sie dort die gewünschten Einstellungen vor.

`.gnu-emacs` definiert die Datei `~/.gnu-emacs-custom` als `custom-file`. Wenn Benutzer in Emacs Einstellungen mit den `customize`-Optionen vornehmen, werden die Einstellungen in `~/.gnu-emacs-custom` gespeichert.

Bei SUSE Linux Enterprise Server wird mit dem `emacs`-Paket die Datei `site-start.el` im Verzeichnis `/usr/share/emacs/site-lisp` installiert. Die Datei `site-start.el` wird vor der Initialisierungsdatei `~/.emacs` geladen. Mit `site-start.el` wird unter anderem sichergestellt, dass spezielle Konfigurationsdateien mit Emacs-Zusatzpaketen, wie `psgml`, automatisch geladen werden. Konfigurationsdateien dieses Typs sind ebenfalls unter `/usr/share/emacs/site-lisp` gespeichert und beginnen immer mit `suse-start-`. Der lokale Systemadministrator kann systemweite Einstellungen in `default.el` festlegen.

Weitere Informationen zu diesen Dateien finden Sie in der Info-Datei zu Emacs unter *Init File*: `info:/emacs/InitFile`. Informationen zum Deaktivieren des Ladens dieser Dateien (sofern erforderlich) stehen dort ebenfalls zur Verfügung.

Die Komponenten von Emacs sind in mehrere Pakete unterteilt:

- Das Basispaket `emacs`.
- `emacs-x11` (in der Regel installiert): das Programm *mit* X11-Support.
- `emacs-nox`: das Programm *ohne* X11-Support.
- `emacs-info`: Online-Dokumentation im info-Format.

- `emacs-el`: die nicht kompilierten Bibliotheksdateien in Emacs Lisp. Sie sind während der Laufzeit nicht erforderlich.
- Verschiedene Add-On-Pakete können bei Bedarf installiert werden: `emacs-auctex` (für LaTeX), `psgml` (für SGML und XML), `gnuserv` (für Client- und Server-Vorgänge) und andere.

9.2 Virtuelle Konsolen

Linux ist ein Multitasking-System für den Mehrbenutzerbetrieb. Die Vorteile dieser Funktionen können auch auf einem eigenständigen PC-System genutzt werden. Im Textmodus stehen sechs virtuelle Konsolen zur Verfügung. Mit den Tastenkombinationen Alt + F1 bis Alt + F6 können Sie zwischen den Konsolen umschalten. Die siebte Konsole ist für X und reserviert und in der zehnten Konsole werden Kernel-Meldungen angezeigt. Durch Ändern der Datei `/etc/inittab` können mehrere oder weniger Konsolen zugewiesen werden.

Wenn Sie von X ohne Herunterfahren zu einer anderen Konsole wechseln möchten, verwenden Sie die Tastenkombinationen Strg + Alt + F1 bis Strg + Alt + F6. Mit Alt + F7 kehren Sie zu X zurück.

9.3 Tastaturzuordnung

Um die Tastaturzuordnung der Programme zu standardisieren, wurden Änderungen an folgenden Dateien vorgenommen:

```
/etc/inputrc
/etc/X11/Xmodmap
/etc/skel/.Xmodmap
/etc/skel/.exrc
/etc/skel/.less
/etc/skel/.lesskey
/etc/csh.cshrc
/etc/termcap
/usr/lib/terminfo/x/xterm
/usr/share/X11/app-defaults/XTerm
/usr/share/emacs/VERSION/site-lisp/term/*.el
```

Diese Änderungen betreffen nur Anwendungen, die `terminfo`-Einträge verwenden oder deren Konfigurationsdateien direkt geändert werden (`vi`, `less` usw.). Anwendun-

gen, die nicht im Lieferumfang des Systems enthalten sind, sollten an diese Standards angepasst werden.

Unter X kann mit der Tastenkombination Strg + Umschalttaste (rechts) auf die Compose-Taste (Multi-Key) zugegriffen werden. Siehe auch den entsprechenden Eintrag in `/etc/X11/Xmodmap`.

Weitere Einstellungen sind mit der X-Tastaturerweiterung (XKB) möglich. Diese Erweiterung wird auch von den Desktop-Umgebungen GNOME (gswitchit) und KDE (kxkb) verwendet.

TIPP: Weiterführende Informationen

Informationen zu XKB finden Sie in `/etc/X11/xkb/README` und den dort aufgeführten Dokumenten.

Detaillierte Informationen zur Eingabe von Chinesisch, Japanisch und Koreanisch (CJK) finden Sie auf der Seite von Mike Fabian: `http://www.suse.de/~mfabian/suse-cjk/input.html`.

9.4 Sprach- und länderspezifische Einstellungen

Das System wurde zu einem großen Teil internationalisiert und kann flexibel an lokale Gegebenheiten angepasst werden. Anders ausgedrückt: Die Internationalisierung (*I18N*) ermöglicht spezielle Lokalisierungen (*L10N*). Die Abkürzungen I18N und L10N wurden von den ersten und letzten Buchstaben der englischsprachigen Begriffe und der Anzahl der dazwischen stehenden ausgelassenen Buchstaben abgeleitet.

Die Einstellungen werden mit `LC_`-Variablen vorgenommen, die in der Datei `/etc/sysconfig/language` definiert sind. Dies bezieht sich nicht nur auf die *native Sprachunterstützung*, sondern auch auf die Kategorien *Meldungen* (Sprache) *Zeichensatz*, *Sortierreihenfolge*, *Uhrzeit und Datum*, *Zahlen* und *Währung*. Diese Kategorien können direkt über eine eigene Variable oder indirekt mit einer Master-Variable in der Datei `language` festgelegt werden (weitere Informationen erhalten Sie auf der Manualpage zu `locale`).

RC_LC_MESSAGES, RC_LC_CTYPE, RC_LC_COLLATE, RC_LC_TIME, RC_LC_NUMERIC, RC_LC_MONETARY
: Diese Variablen werden ohne das Präfix RC_ an die Shell weitergegeben und stehen für die aufgelisteten Kategorien. Die betreffenden Shell-Profile werden unten aufgeführt. Die aktuelle Einstellung lässt sich mit dem Befehl locale anzeigen.

RC_LC_ALL
: Sofern diese Variable festgelegt ist, setzt Sie die Werte der bereits erwähnten Variablen außer Kraft.

RC_LANG
: Falls keine der zuvor genannten Variablen festgelegt ist, ist dies das Fallback. Standardmäßig wird nur RC_LANG festgelegt. Dadurch wird es für die Benutzer einfacher, eigene Werte einzugeben.

ROOT_USES_LANG
: Eine Variable, die entweder den Wert yes oder den Wert no aufweist. Wenn die Variable auf no gesetzt ist, funktioniert root immer in der POSIX-Umgebung.

Die Variablen können über den sysconfig-Editor von YaST (siehe Abschnitt 7.3.1, „Ändern der Systemkonfiguration mithilfe des YaST-Editors "sysconfig"“ (S. 80)) festgelegt werden. Der Wert einer solchen Variable enthält den Sprachcode, den Ländercode, die Codierung und einen Modifier. Die einzelnen Komponenten werden durch Sonderzeichen verbunden:

```
LANG=<language>[[_<COUNTRY>].<Encoding>[@<Modifier>]]
```

9.4.1 Beispiele

Sprach- und Ländercode sollten immer gleichzeitig eingestellt werden. Die Spracheinstellungen entsprechen der Norm ISO 639, die unter http://www.evertype.com/standards/iso639/iso639-en.html und http://www.loc.gov/standards/iso639-2/ verfügbar ist. Die in ISO 3166 aufgeführten Ländercodes sind unter http://www.din.de/gremien/nas/nabd/iso3166ma/codlstp1/en_listp1.html verfügbar.

Es ist nur sinnvoll, Werte festzulegen, für die verwendbare Beschreibungsdateien unter /usr/lib/locale zu finden sind. Anhand der Dateien in /usr/share/i18n

können mit dem Befehl `localedef` zusätzliche Beschreibungsdateien erstellt werden. Die Beschreibungsdateien sind Bestandteil des Pakets `glibc-i18ndata`. Eine Beschreibungsdatei für `en_US.UTF-8` (für Englisch und USA) kann beispielsweise wie folgt erstellt werden:

```
localedef -i en_US -f UTF-8 en_US.UTF-8
```

`LANG=en_US.UTF-8`
: Dies ist die Standardeinstellung, wenn während der Installation US-Englisch ausgewählt wurde. Wenn Sie eine andere Sprache ausgewählt haben, wird diese Sprache ebenfalls mit der Zeichencodierung UTF-8 aktiviert.

`LANG=en_US.ISO-8859-1`
: Hiermit wird als Sprache Englisch, als Land die USA und als Zeichensatz `ISO-8859-1` festgelegt. In diesem Zeichensatz wird das Eurozeichen nicht unterstützt, es kann jedoch gelegentlich in Programmen nützlich sein, die nicht für die `UTF-8`-Unterstützung aktualisiert wurden. Die Zeichenkette, mit der der Zeichensatz definiert wird (in diesem Fall `ISO-8859-1`), wird anschließend von Programmen, wie Emacs, ausgewertet.

`LANG=en_IE@euro`
: Im oben genannten Beispiel wird das Eurozeichen explizit in die Spracheinstellung aufgenommen. Streng genommen ist diese Einstellung mittlerweile veraltet, da das Eurozeichen jetzt ebenfalls in UTF-8 enthalten ist. Diese Einstellung ist nur sinnvoll, wenn eine Anwendung UTF-8 nicht unterstützt, ISO-8859-15 jedoch unterstützt.

SuSEconfig liest die Variablen in `/etc/sysconfig/language` und speichert die erforderlichen Änderungen in `/etc/SuSEconfig/profile` und `/etc/SuSEconfig/csh.cshrc`. `/etc/SuSEconfig/profile` von `/etc/profile` gelesen oder als *Quelle verwendet*. `/etc/SuSEconfig/csh.cshrc` wird von `/etc/csh.cshrc` als Quelle verwendet. Auf diese Weise werden die Einstellungen systemweit verfügbar.

Die Benutzer können die Standardeinstellungen des Systems außer Kraft setzen, indem Sie die Datei `~/.bashrc` entsprechend bearbeiten. Wenn Sie die systemübergreifende Einstellung `en_US` für Programmmeldungen beispielsweise nicht verwenden möchten, nehmen Sie beispielsweise `LC_MESSAGES=es_ES` auf, damit die Meldungen stattdessen auf Spanisch angezeigt werden.

9.4.2 Locale-Einstellungen in ~/.i18n

Wenn Sie mit den Locale-Systemstandardwerten nicht zufrieden sind, können Sie die Einstellungen in `~/.i18n` ändern. Achten Sie dabei jedoch auf die Einhaltung der Bash-Scripting-Syntax. Die Einträge in `~/.i18n` setzen die Systemstandardwerte aus `/etc/sysconfig/language` außer Kraft. Verwenden Sie dieselben Variablennamen, jedoch ohne die `RC_`-Präfixe für den Namespace, also beispielsweise `LANG` anstatt `RC_LANG`:

```
LANG=cs_CZ.UTF-8
LC_COLLATE=C
```

9.4.3 Einstellungen für die Sprachunterstützung

Die Dateien in der Kategorie *Meldungen* werden generell im entsprechenden Sprachverzeichnis (wie beispielsweise `en`) gespeichert, damit ein Fallback vorhanden ist. Wenn Sie für `LANG` den Wert `en_US` festlegen und in `/usr/share/locale/en_US/LC_MESSAGES` keine Meldungsdatei vorhanden ist, wird ein Fallback auf `/usr/share/locale/en/LC_MESSAGES` ausgeführt.

Darüber hinaus kann eine Fallback-Kette definiert werden, beispielsweise für Bretonisch zu Französisch oder für Galizisch zu Spanisch oder Portugiesisch:

```
LANGUAGE="br_FR:fr_FR"
```

```
LANGUAGE="gl_ES:es_ES:pt_PT"
```

Wenn Sie möchten, können Sie die norwegischen Varianten Nynorsk und Bokmål (mit zusätzlichem Fallback auf `no`) verwenden:

```
LANG="nn_NO"
```

```
LANGUAGE="nn_NO:nb_NO:no"
```

oder

```
LANG="nb_NO"
```

```
LANGUAGE="nb_NO:nn_NO:no"
```

Beachten Sie, das bei Norwegisch auch `LC_TIME` anders behandelt wird.

Ein mögliches Problem ist, dass ein Trennzeichen, das zum Trennen von Zifferngruppen verwendet wird, nicht richtig erkannt wird. Dies passiert, wenn `LANG` auf einen aus zwei Buchstaben bestehenden Sprachcode wie `de` eingestellt ist, die Definitionsdatei, die glibc verwendet, jedoch in `/usr/share/lib/de_DE/LC_NUMERIC` gespeichert ist. Daher muss `LC_NUMERIC` auf `de_DE` gesetzt sein, damit das System die Trennzeichendefinition erkennen kann.

9.4.4 Weiterführende Informationen

- *The GNU C Library Reference Manual*, Kapitel "Locales and Internationalization". Dieses Handbuch ist in `glibc-info` enthalten.
- Markus Kuhn, *UTF-8 and Unicode FAQ for Unix/Linux*, momentan verfügbar unter `http://www.cl.cam.ac.uk/~mgk25/unicode.html`.
- *Unicode-Howto*, von Bruno Haible: `/usr/share/doc/howto/en/html/Unicode-HOWTO.html`.

10 Druckerbetrieb

SUSE® Linux Enterprise Server unterstützt viele Arten von Druckern, einschließlich Remote- und Netzwerkdrucker. Drucker können mit YaST oder manuell konfiguriert werden. Anleitungen zur Konfiguration finden Sie unter Abschnitt „Einrichten eines Druckers“ (Kapitel 8, *Einrichten von Hardware-Komponenten mit YaST*, ↑*Bereitstellungshandbuch*). Grafische Dienstprogramme und Dienstprogramme an der Kommandozeile sind verfügbar, um Druckaufträge zu starten und zu verwalten. Wenn Ihr Drucker nicht wie erwartet verwendet werden kann, lesen Sie die Informationen unter Abschnitt 10.8, „Fehlersuche“ (S. 134).

CUPS ist das Standard-Drucksystem in SUSE Linux Enterprise Server. CUPS ist stark benutzerorientiert. In vielen Fällen ist es kompatibel mit LPRng oder kann mit relativ geringem Aufwand angepasst werden. LPRng ist lediglich aus Kompatibilitätsgründen im Lieferumfang von SUSE Linux Enterprise Server enthalten.

Drucker können nach Schnittstelle, z. B. USB oder Netzwerk, und nach Druckersprache unterschieden werden. Stellen Sie beim Kauf eines Druckers sicher, dass der Drucker über eine für Ihre Hardware geeignete Schnittstelle (wie USB oder einen parallelen Port) und eine geeignete Druckersprache verfügt. Drucker können basierend auf den folgenden drei Klassen von Druckersprachen kategorisiert werden:

PostScript-Drucker
: PostScript ist die Druckersprache, in der die meisten Druckaufträge unter Linux und Unix vom internen Drucksystem generiert und verarbeitet werden. Diese Sprache ist sehr alt und sehr effizient. Wenn PostScript-Dokumente direkt vom Drucker verarbeitet und im Drucksystem nicht in weiteren Phasen konvertiert werden müssen, reduziert sich die Anzahl der möglichen Fehlerquellen. Da Post-

Script-Drucker immer mit erheblichen Lizenzkosten verbunden sind, sind diese Drucker in der Regel teurer als Drucker ohne PostScript-Interpreter.

Standarddrucker (Sprachen wie PCL und ESC/P)
: Obwohl diese Druckersprachen ziemlich alt sind, werden sie immer weiter entwickelt, um neue Druckerfunktionen unterstützen zu können. Bei den bekannten Druckersprachen kann das Drucksystem PostScript-Druckaufträge mithilfe von Ghostscript in die entsprechende Druckersprache konvertieren. Diese Verarbeitungsphase wird als "Interpretieren" bezeichnet. Die gängigsten Sprachen sind PCL, die am häufigsten auf HP-Druckern und ihren Klonen zum Einsatz kommt, und ESC/P, die bei Epson-Druckern verwendet wird. Diese Druckersprachen werden in der Regel von Linux unterstützt und liefern ein annehmbares Druckergebnis. Es kann sein, dass Linux einige neue Drucker mit sehr ausgefallenen Funktionen nicht unterstützt, da die Open-Source-Entwickler möglicherweise an diesen Funktionen noch arbeiten. Mit Ausnahme der von HP entwickelten HPLIP gibt es derzeit keinen Druckerhersteller, der Linux-Treiber entwickeln und sie den Linux-Distributoren unter einer Open-Source-Lizenz zur Verfügung stellen würde. Die meisten dieser Drucker finden sich im mittleren Preisbereich.

Proprietäre Drucker (auch GDI-Drucker genannt)
: Diese Drucker unterstützen keine der gängigen Druckersprachen. Sie verwenden eigene, undokumentierte Druckersprachen, die geändert werden können, wenn neue Versionen eines Modells auf den Markt gebracht werden. Für diese Drucker sind in der Regel nur Windows-Treiber verfügbar. Weitere Informationen finden Sie unter Abschnitt 10.8.1, „Drucker ohne Unterstützung für eine Standard-Druckersprache“ (S. 134).

Vor dem Kauf eines neuen Druckers sollten Sie anhand der folgenden Quellen prüfen, wie gut der Drucker, den Sie zu kaufen beabsichtigen, unterstützt wird:

`http://www.linuxfoundation.org/en/OpenPrinting/`
: Die OpenPrinting.org-Druckerdatenbank

`http://www.cs.wisc.edu/~ghost/`
: Die Ghostscript-Website

`/usr/share/doc/packages/ghostscript-library/catalog.devices`
: Liste inbegriffener Treiber.

In den Online-Datenbanken wird immer der neueste Linux-Supportstatus angezeigt. Eine Linux-Distribution kann jedoch immer nur die zur Produktionszeit verfügbaren Treiber enthalten. Demnach ist es möglich, dass ein Drucker, der aktuell als "vollständig unterstützt" eingestuft wird, diesen Status bei der Veröffentlichung der neuesten SUSE Linux Enterprise Server-Version nicht aufgewiesen hat. Die Datenbank gibt daher nicht notwendigerweise den richtigen Status, sondern nur eine Annäherung an diesen an.

10.1 Work-Flow des Drucksystems

Der Benutzer erstellt einen Druckauftrag. Der Druckauftrag besteht aus den zu druckenden Daten sowie aus Informationen für den Spooler, z. B. dem Namen des Druckers oder dem Namen der Druckwarteschlange und - optional - den Informationen für den Filter, z. B. druckerspezifische Optionen.

Mindestens eine zugeordnete Druckerwarteschlange ist für jeden Drucker vorhanden. Der Spooler hält den Druckauftrag in der Warteschlange, bis der gewünschte Drucker bereit ist, Daten zu empfangen. Wenn der Drucker druckbereit ist, sendet der Spooler die Daten über den Filter und das Backend an den Drucker.

Der Filter konvertiert die von der druckenden Anwendung generierten Daten (in der Regel PostScript oder PDF, aber auch ASCII, JPEG usw.) in druckerspezifische Daten (PostScript, PCL, ESC/P usw.). Die Funktionen des Druckers sind in den PPD-Dateien beschrieben. Eine PPD-Datei enthält druckspezifische Optionen mit den Parametern, die erforderlich sind, um die Optionen auf dem Drucker zu aktivieren. Das Filtersystem stellt sicher, dass die vom Benutzer ausgewählten Optionen aktiviert werden.

Wenn Sie einen PostScript-Drucker verwenden, konvertiert das Filtersystem die Daten in druckerspezifische PostScript-Daten. Hierzu ist kein Druckertreiber erforderlich. Wenn Sie einen Nicht-PostScript-Drucker verwenden, konvertiert das Filtersystem die Daten in druckerspezifische Daten. Hierzu ist ein für den Drucker geeigneter Druckertreiber erforderlich. Das Back-End empfängt die druckerspezifischen Daten vom Filter und leitet sie an den Drucker weiter.

10.2 Methoden und Protokolle zum Anschließen von Druckern

Es gibt mehrere Möglichkeiten, einen Drucker an das System anzuschließen. Die Konfiguration des CUPS-Drucksystems unterscheidet nicht zwischen einem lokalen Drucker und einem Drucker, der über das Netzwerk an das System angeschlossen ist. Unter Linux müssen lokale Drucker wie im Handbuch des Druckerherstellers beschrieben angeschlossen werden. CUPS unterstützt serielle, USB-, Parallel- und SCSI-Verbindungen.

► **zseries:** Von der z/VM bereitgestellte Drucker und ähnliche Geräte, die Sie lokal an IBM-System z-Mainframes anschließen können, werden von CUPS und LPRng nicht unterstützt. Auf diesen Plattformen ist das Drucken nur über das Netzwerk möglich. Die Kabel für Netzwerkdrucker müssen gemäß den Anleitungen des Druckerherstellers angeschlossen werden. ◄

WARNUNG: Ändern der Anschlüsse bei einem laufenden System

Vergessen Sie beim Anschließen des Druckers an den Computer nicht, dass während des Betriebs nur USB-Geräte angeschlossen werden können. Um Ihr System oder Ihren Drucker vor Schaden zu bewahren, fahren Sie das System herunter, wenn Sie Verbindungen ändern müssen, die keine USB-Verbindungen sind.

10.3 Installation der Software

PPD (PostScript Printer Description, PostScript-Druckerbeschreibung) ist die Computersprache, die die Eigenschaften, z. B. die Auflösung und Optionen wie die Verfügbarkeit einer Duplexeinheit, beschreibt. Diese Beschreibungen sind für die Verwendung der unterschiedlichen Druckeroptionen in CUPS erforderlich. Ohne eine PPD-Datei würden die Druckdaten in einem "rohen" Zustand an den Drucker weitergeleitet werden, was in der Regel nicht erwünscht ist. Während der Installation von SUSE Linux Enterprise Server werden viele PPD-Dateien vorinstalliert.

Um einen PostScript-Drucker zu konfigurieren, sollten Sie sich zunächst eine geeignete PPD-Datei beschaffen. Viele PPD-Dateien sind im Paket `manufacturer-PPDs`

enthalten, das im Rahmen der Standardinstallation automatisch installiert wird. Weitere Informationen hierzu finden Sie unter Abschnitt 10.7.2, „PPD-Dateien in unterschiedlichen Paketen“ (S. 132) und Abschnitt 10.8.2, „Für einen PostScript-Drucker ist keine geeignete PPD-Datei verfügbar“ (S. 135).

Neue PPD-Dateien können im Verzeichnis `/usr/share/cups/model/` gespeichert oder dem Drucksystem mit YaST hinzugefügt werden (siehe „Hinzufügen von Treibern mit YaST“ (Kapitel 8, *Einrichten von Hardware-Komponenten mit YaST*, ↑*Bereitstellungshandbuch*)). Die PPD-Dateien lassen sich anschließend während der Installation auswählen.

Seien Sie vorsichtig, wenn ein Druckerhersteller verlangt, dass Sie zusätzlich zum Ändern der Konfigurationsdateien vollständige Softwarepakte installieren sollen. Diese Art der Installation würde erstens dazu führen, dass Sie die Unterstützung von SUSE Linux Enterprise Server verlieren, und zweitens können Druckbefehle anders funktionieren und das System ist möglicherweise nicht mehr in der Lage, Geräte anderer Hersteller anzusprechen. Aus diesem Grund wird das Installieren von Herstellersoftware nicht empfohlen.

10.4 Netzwerkdrucker

Ein Netzwerkdrucker kann unterschiedliche Protokolle unterstützen - einige von diesen sogar gleichzeitig. Obwohl die meisten der unterstützten Protokolle standardisiert sind, erweitern (ändern) einige Hersteller den Standard, weil sie Systeme testen, die in den Standard noch nicht ordnungsgemäß implementiert wurden, oder weil sie bestimmte Funktionen zur Verfügung stellen möchten, die im Standard nicht enthalten sind. Hersteller stellen in diesem Fall nur für wenige Betriebssysteme Treiber zur Verfügung und eliminieren so die Schwierigkeiten mit diesen Systemen. Linux-Treiber werden leider nur sehr selten zur Verfügung gestellt. Gegenwärtig können Sie nicht davon ausgehen, dass alle Protokolle problemlos mit Linux funktionieren. Um dennoch eine funktionale Konfiguration zu erhalten, müssen Sie daher möglicherweise mit den verschiedenen Optionen experimentieren.

CUPS unterstützt die Protokolle `socket`, `LPD`, `IPP` und `smb`.

socket
: *Socket* bezieht sich auf eine Verbindung, in der die Daten an ein Internet-Socket gesendet werden, ohne dass zuvor ein Data-Handshake erfolgt. Einige der am

häufigsten verwendeten Socket-Ports sind `9100` oder `35`. Die Syntax der Geräte-URI (Uniform Resource Identifier) ist socket://*`IP.of.the.printer`*:*`port`*, zum Beispiel `socket://192.168.2.202:9100/`.

LPD (Line Printer Daemon)
: Das bewährte LPD-Protokoll wird in RFC 1179 beschrieben. Mit diesem Protokoll werden einige druckauftragsbezogene Daten, z. B. die ID der Druckwarteschlange, vor den eigentlichen Druckdaten gesendet. Daher muss die Druckwarteschlange beim Konfigurieren des LPD-Protokolls für die Datenübertragung angegeben werden. Die Implementierungen diverser Druckerhersteller sind flexibel genug, um beliebige Namen als Druckwarteschlange zu akzeptieren. Der zu verwendende Name müsste ggf. im Druckerhandbuch angegeben sein. Es werden häufig Bezeichnungen wie LPT, LPT1, LP1 o. ä. verwendet. Eine LPD-Warteschlange kann auch auf einem anderen Linux- oder Unix-Host im CUPS-System konfiguriert werden. Die Portnummer für einen LPD-Dienst lautet `515`. Ein Beispiel für einen Gerät-URI ist `lpd://192.168.2.202/LPT1`.

IPP (Internet Printing Protocol)
: IPP ist ein relativ neues Protokoll (1999), das auf dem HTTP-Protokoll basiert. Mit IPP können mehr druckauftragsbezogene Daten übertragen werden als mit den anderen Protokollen. CUPS verwendet IPP für die interne Datenübertragung. Dies ist das bevorzugte Protokoll für eine Weiterleitungswarteschlange zwischen zwei CUPS-Servern. Um IPP ordnungsgemäß konfigurieren zu können, ist der Name der Druckwarteschlange erforderlich. Die Portnummer für IPP lautet `631`. Beispiele für Geräte-URIs sind `ipp://192.168.2.202/ps` und `ipp://192.168.2.202/printers/ps`.

SMB (Windows-Freigabe)
: CUPS unterstützt auch das Drucken auf freigegebenen Druckern unter Windows. Das für diesen Zweck verwendete Protokoll ist SMB. SMB verwendet die Portnummern `137`, `138` und `139`. Beispiele für Geräte-URIs sind `smb://user:password@workgroup/smb.example.com/printer`, `smb://user:password@smb.example.com/printer` und `smb://smb.example.com/printer`.

Das vom Drucker unterstützte Protokoll muss vor der Konfiguration ermittelt werden. Wenn der Hersteller die erforderlichen Informationen nicht zur Verfügung stellt, können Sie das Protokoll mit dem Befehl `nmap` ermitteln, der Bestandteil des Pakets `nmap` ist. `nmap` überprüft einen Host auf offene Ports. Beispiel:

```
nmap -p 35,137-139,515,631,9100-10000 printerIP
```

10.4.1 Konfigurieren von CUPS mit Kommandozeilenwerkzeugen

Sie können beim Konfigurieren eines Netzwerkdruckers die CUPS-Optionen nicht nur mit YaST einstellen, sondern können auch auf Kommandozeilenwerkzeuge wie `lpadmin` und `lpoptions` zugreifen. Sie benötigen ein Geräte-URI, das aus einem Backend, z. B. parallel, und Parametern besteht. Zum Bestimmen von gültigen Geräte-URIs auf Ihrem System verwenden Sie das Kommando `lpinfo -v | grep ":/"`:

```
# lpinfo -v | grep ":/"
direct usb://ACME/FunPrinter%20XL
direct parallel:/dev/lp0
```

Mit `lpadmin` kann der CUPS-Serveradministrator Klassen und Druckwarteschlangen hinzufügen, entfernen und verwalten. Verwenden Sie die folgende Syntax, um eine Druckwarteschlange hinzuzufügen:

```
lpadmin -p queue -v device-URI -P PPD-file -E
```

Das Gerät (`-v`) ist anschließend als *`Warteschlange`* (`-p`) verfügbar und verwendet die angegebene PPD-Datei (`-P`). Das bedeutet, dass Sie die PPD-Datei und das Geräte-URI kennen müssen, wenn Sie den Drucker manuell konfigurieren möchten.

Verwenden Sie nicht `-E` als erste Option. Für alle CUPS-Befehle legt die Option `-E` als erstes Argument die Verwendung einer verschlüsselten Verbindung fest. Zur Aktivierung des Druckers muss die Option `-E` wie im folgenden Beispiel dargestellt verwendet werden:

```
lpadmin -p ps -v parallel:/dev/lp0 -P \
/usr/share/cups/model/Postscript.ppd.gz -E
```

Im folgenden Beispiel wird ein Netzwerkdrucker konfiguriert:

```
lpadmin -p ps -v socket://192.168.2.202:9100/ -P \
/usr/share/cups/model/Postscript-level1.ppd.gz -E
```

Weitere Optionen von `lpadmin` finden Sie auf der man-Seiten von `lpadmin(1)`.

Während der Druckerkonfiguration werden bestimmte Optionen standardmäßig gesetzt. Diese Optionen können (je nach Druckwerkzeug) für jeden Druckauftrag geändert

werden. Es ist auch möglich, diese Standardoptionen mit YaST zu ändern. Legen Sie die Standardoptionen mithilfe der Kommandozeilenwerkzeuge wie folgt fest:

1. Zeigen Sie zunächst alle Optionen an:

   ```
   lpoptions -p queue -l
   ```

   Beispiel:

   ```
   Resolution/Output Resolution: 150dpi *300dpi 600dpi
   ```

   Die aktivierte Standardoption wird durch einen vorangestellten Stern (`*`) gekennzeichnet.

2. Ändern Sie die Option mit `lpadmin`:

   ```
   lpadmin -p queue -o Resolution=600dpi
   ```

3. Prüfen Sie die neue Einstellung:

   ```
   lpoptions -p queue -l

   Resolution/Output Resolution: 150dpi 300dpi *600dpi
   ```

Wenn ein normaler Benutzer `lpoptions` ausführt, werden die Einstellungen in `~/.cups/lpoptions` geschrieben. Jedoch werden die `root`-Einstellungen in to `/etc/cups/lpoptions` geschrieben.

10.5 Grafische Bedienoberflächen für das Drucken

Werkzeuge wie xpp und das KDE-Programm KPrinter bieten eine grafische Oberfläche für die Auswahl der Warteschlangen und zum Festlegen der CUPS-Standardoptionen und druckerspezifischen Optionen, die über die PPD-Datei zur Verfügung gestellt werden. Sie können KPrinter sogar als Standard-Druckoberfläche für Nicht-KDE-Anwendungen benutzen. Geben Sie im Druckdialogfeld dieser Anwendungen `kprinter` oder `kprinter--stdin` als Druckbefehl an. Das geeignete Kommando hängt davon ab, wie die Anwendung die Daten überträgt. Probieren Sie einfach aus, welches Kommando funktioniert. Wenn die Anwendung ordnungsgemäß konfiguriert ist, sollte bei jedem Druckauftrag das Dialogfeld "KPrinter" geöffnet werden, in dem

Sie eine Warteschlange wählen und andere Druckoptionen festlegen können. Hierfür dürfen keine Konflikte zwischen den Druckereinstellungen der Anwendung und KPrinter auftreten. Die Druckoptionen dürfen nur über KPrinter geändert werden, nachdem das Programm aktiviert wurde.

10.6 Drucken über die Kommandozeile

Um den Druckvorgang über die Kommandozeile zu starten, geben Sie `lp -d` *`Name_der_WarteschlangeDateiname`* ein und ersetzen die entsprechenden Namen für *`Name_der_Warteschlange`* und *`Dateiname`*.

Einige Anwendungen erfordern für den Druckvorgang den Befehl `lp`. Geben Sie in diesem Fall den richtigen Befehl in das Druckdialogfeld der Anwendung ohne Angabe des *`Dateinamens`* ein, z. B. `lp -d` *`Name_der_Warteschlange`*.

10.7 Spezielle Funktionen in SUSE Linux Enterprise Server

Für SUSE Linux Enterprise Server wurden mehrere CUPS-Funktionen angepasst. Im Folgenden werden einige der wichtigsten Änderungen beschrieben.

10.7.1 CUPS und Firewall

Nach einer Standardinstallation von SUSE Linux Enterprise Server ist SuSEfirewall2 aktiv, und die externen Netzwerkschnittstellen sind in der `externen Zone` konfiguriert, die eingehenden Datenverkehr blockiert. Diese Standardeinstellungen müssen geändert werden, wenn Sie CUPS verwenden wollen. Weitere Informationen zur SUSEfirewall2-Konfiguration finden Sie unter Abschnitt „SuSEfirewall2“ (Kapitel 8, *Masquerading and Firewalls*, ↑*Security Guide*).

CUPS-Client

Normalerweise wird der CUPS-Client auf einem normalen Arbeitsplatzrechner ausgeführt, die sich in einer verbürgten Netzwerkumgebung hinter einer Firewall befindet. In diesem Fall empfiehlt es sich, die Netzwerkschnittstelle in der `internen Zone` zu konfigurieren, damit der Arbeitsplatzrechner innerhalb des Netzwerks erreichbar ist.

CUPS-Server

Wenn der CUPS-Server Teil der durch eine Firewall geschützten verbürgten Netzwerkumgebung ist, sollte die Netzwerkschnittstelle in der `internen Zone` der Firewall konfiguriert sein. Es ist nicht empfehlenswert, einen CUPS-Server in einer nicht verbürgten Netzwerkumgebung einzurichten, es sei denn, Sie sorgen dafür, dass er durch besondere Firewall-Regeln und Sicherheitseinstellungen in der CUPS-Konfiguration geschützt wird.

10.7.2 PPD-Dateien in unterschiedlichen Paketen

Die YaST-Druckerkonfiguration richtet die Warteschlangen für CUPS auf dem System nur mit den in `/usr/share/cups/model/` installierten PPD-Dateien ein. Um die geeigneten PPD-Dateien für das Druckermodell zu finden, vergleicht YaST während der Hardware-Erkennung den Hersteller und das Modell mit den Herstellern und Modellen, die auf dem System in den PPD-Dateien unter `/usr/share/cups/model/` verfügbar sind. Zu diesem Zweck generiert die YaST-Druckerkonfiguration eine Datenbank mit den Hersteller- und Modelldaten, die aus den PPD-Dateien extrahiert werden. Wenn Sie einen Drucker auswählen, empfangen Sie die PPD-Dateien, die dem Hersteller und dem Modell aus der Liste der Modelle entsprechen.

Die Konfiguration, die nur PPD-Dateien und keine weiteren Informationsquellen verwendet, hat den Vorteil, dass die PPD-Dateien in `/usr/share/cups/model/` beliebig geändert werden können. Die YaST-Druckerkonfiguration erkennt die Änderungen und generiert die Hersteller- und Modelldatenbank neu. Wenn Sie beispielsweise nur mit PostScript-Druckern arbeiten, sind die Foomatic-PPD-Dateien im Paket `cups-drivers` oder die Gutenprint-PPD-Dateien im Paket `gutenprint` in der Regel nicht erforderlich. Stattdessen können die PPD-Dateien für die PostScript-Drucker

direkt in /usr/share/cups/model/ kopiert werden (wenn sie nicht bereits im Paket manufacturer-PPDs vorhanden sind), um eine optimale Konfiguration der Drucker zu erzielen.

CUPS-PPD-Dateien im Paket cups

Die generischen PPD-Dateien im Paket cups wurden durch angepasste Foomatic-PPD-Dateien für PostScript-Drucker der Level 1 und Level 2 ergänzt:

- /usr/share/cups/model/Postscript-level1.ppd.gz
- /usr/share/cups/model/Postscript-level2.ppd.gz

PPD-Dateien im Paket cups-drivers

Der Foomatic-Druckerfilter foomatic-rip wird in der Regel zusammen mit Ghostscript für Nicht-PostScript-Drucker verwendet. Geeignete Foomatic PPD-Dateien haben die Einträge *NickName: ... Foomatic/Ghostscript driver und *cupsFilter: ... foomatic-rip. Diese PPD-Dateien befinden sich im Paket cups-drivers.

YaST bevorzugt in der Regel eine Hersteller-PPD-Datei. Wenn jedoch keine passende Hersteller-PPD-Datei existiert, wird eine Foomatic-PPD-Datei mit dem Eintrag *Spitzname: ... Foomatic ... (empfohlen) ausgewählt.

Gutenprint-PPD-Dateien im gutenprint-Paket

Für viele Nicht-PostScript-Drucker kann anstelle von foomatic-rip der CUPS-Filter rastertogutenprint von Gutenprint (früher GIMP-Print) verwendet werden. Dieser Filter und die entsprechenden Gutenprint-PPD-Dateien befinden sich im Paket gutenprint. Die Gutenprint-PPD-Dateien befinden sich in /usr/share/cups/model/gutenprint/ und haben die Einträge *Spitzname: ... CUPS+Gutenprint und *cupsFilter: ... rastertogutenprint.

PPD-Dateien von Druckerherstellern im Paket `manufacturer-PPDs`

Das Paket `manufacturer-PPDs` enthält PPD-Dateien von Druckerherstellern, die unter einer ausreichend freien Lizenz veröffentlicht werden. PostScript-Drucker sollten mit der entsprechenden PPD-Datei des Druckerherstellers konfiguriert werden, da diese Datei die Verwendung aller Funktionen des PostScript-Druckers ermöglicht. YaST bevorzugt eine PPD-Datei aus den `Hersteller-PPDs`. YaST kann keine PPD-Datei aus dem Paket der `Hersteller-PPDs` verwenden, wenn der Modellname nicht übereinstimmt. Dies kann geschehen, wenn das Paket der `Hersteller-PPDs` nur eine PPD-Datei für ähnliche Modelle enthält, z. B. Funprinter 12xx-Serie. Wählen Sie in diesem Fall die enstprechende PPD-Datei manuell in YaST aus.

10.8 Fehlersuche

In den folgenden Abschnitten werden einige der am häufigsten auftretenden Probleme mit der Druckerhardware und -software sowie deren Lösungen oder Umgehung beschrieben. Unter anderem werden die Themen GDI-Drucker, PPD-Dateien und Port-Konfiguration behandelt. Darüber hinaus werden gängige Probleme mit Netzwerkdruckern, fehlerhafte Ausdrucke und die Bearbeitung der Warteschlange erläutert.

10.8.1 Drucker ohne Unterstützung für eine Standard-Druckersprache

Diese Drucker unterstützen keine der geläufigen Druckersprachen und können nur mit proprietären Steuersequenzen adressiert werden. Daher funktionieren sie nur mit den Betriebssystemversionen, für die der Hersteller einen Treiber zur Verfügung stellt. GDI ist eine von Microsoft für Grafikgeräte entwickelte Programmierschnittstelle. In der Regel liefert der Hersteller nur Treiber für Windows. Da die Windows-Treiber die GDI-Schnittstelle verwenden, werden diese Drucker auch *GDI-Drucker* genannt. Das eigentliche Problem ist nicht die Programmierschnittstelle, sondern die Tatsache, dass diese Drucker nur mit der proprietären Druckersprache des jeweiligen Druckermodells adressiert werden können.

Der Betrieb einiger GDI-Drucker kann sowohl im GDI-Modus als auch in einer der Standard-Druckersprachen ausgeführt werden. Sehen Sie im Druckerhandbuch nach, ob dies möglich ist. Einige Modelle benötigen für diese Umstellung eine spezielle Windows-Software (Beachten Sie, dass der Windows-Druckertreiber den Drucker immer zurück in den GDI-Modus schalten kann, wenn von Windows aus gedruckt wird). Für andere GDI-Drucker sind Erweiterungsmodule für eine Standarddruckersprache erhältlich.

Einige Hersteller stellen für ihre Drucker proprietäre Treiber zur Verfügung. Der Nachteil proprietärer Druckertreiber ist, dass es keine Garantie gibt, dass diese mit dem installierten Drucksystem funktionieren und für die unterschiedlichen Hardwareplattformen geeignet sind. Im Gegensatz dazu sind Drucker, die eine Standard-Druckersprache unterstützen, nicht abhängig von einer speziellen Drucksystemversion oder einer bestimmten Hardwareplattform.

Anstatt Zeit darauf zu verwenden, einen proprietären Linux-Treiber zum Funktionieren zu bringen, ist es möglicherweise kosteneffektiver, einen unterstützten Drucker zu kaufen. Dadurch wäre das Treiberproblem ein für alle Mal aus der Welt geschafft und es wäre nicht mehr erforderlich, spezielle Treibersoftware zu installieren und zu konfigurieren oder Treiber-Updates zu beschaffen, die aufgrund neuer Entwicklungen im Drucksystem benötigt würden.

10.8.2 Für einen PostScript-Drucker ist keine geeignete PPD-Datei verfügbar

Wenn das Paket `manufacturer-PPDs` für einen PostScript-Drucker keine geeignete PPD-Datei enthält, sollte es möglich sein, die PPD-Datei von der Treiber-CD des Druckerherstellers zu verwenden, oder eine geeignete PPD-Datei von der Webseite des Druckerherstellers herunterzuladen.

Wenn die PPD-Datei als Zip-Archiv (.zip) oder als selbstextrahierendes Zip-Archiv (`.exe`) zur Verfügung gestellt wird, entpacken Sie sie mit `unzip`. Lesen Sie zunächst die Lizenzvereinbarung für die PPD-Datei. Prüfen Sie dann mit dem Dienstprogramm `cupstestppd`, ob die PPD-Datei den Spezifikationen "Adobe PostScript Printer Description File Format Specification, Version 4.3." entspricht. Wenn das Dienstprogramm "FAIL" zurückgibt, sind die Fehler in den PPD-Dateien schwerwiegend und werden sehr wahrscheinlich größere Probleme verursachen. Die von `cupstestppd`

protokollierten Problempunkte müssen behoben werden. Fordern Sie beim Druckerhersteller ggf. eine geeignete PPD-Datei an.

10.8.3 Parallele Anschlüsse

Die sicherste Methode ist, den Drucker direkt an den ersten Parallelanschluss anzuschließen und im BIOS die folgenden Einstellungen für Parallelanschlüsse auszuwählen:

- E/A-Adresse: `378` (hexadezimal)
- Interrupt: nicht relevant
- Modus: `Normal`, `SPP` oder `Nur Ausgabe`
- DMA: deaktiviert

Wenn der Drucker trotz dieser Einstellungen über den Parallelanschluss nicht angesprochen werden kann, geben Sie die E/A-Adresse explizit entsprechend den Einstellungen im BIOS in der Form `0x378` in `/etc/modprobe.conf` ein. Wenn zwei Parallelanschlüsse vorhanden sind, die auf die E/A-Adressen `378` und `278` (hexadezimal) gesetzt sind, geben Sie diese in Form von `0x378,0x278` ein.

Wenn Interrupt `7` frei ist, kann er mit dem in Beispiel 10.1, „`/etc/modprobe.conf`: Interrupt-Modus für den ersten parallelen Port“ (S. 136) dargestellten Eintrag aktiviert werden. Prüfen Sie vor dem Aktivieren des Interrupt-Modus die Datei `/proc/interrupts`, um zu sehen, welche Interrupts bereits verwendet werden. Es werden nur die aktuell verwendeten Interrupts angezeigt. Dies kann sich je nachdem, welche Hardwarekomponenten aktiv sind, ändern. Der Interrupt für den Parallelanschluss darf von keinem anderen Gerät verwendet werden. Wenn Sie sich diesbezüglich nicht sicher sind, verwenden Sie den Polling-Modus mit `irq=none`.

Beispiel 10.1 *`/etc/modprobe.conf`: Interrupt-Modus für den ersten parallelen Port*

```
alias parport_lowlevel parport_pc
options parport_pc io=0x378 irq=7
```

10.8.4 Netzwerkdrucker-Verbindungen

Netzwerkprobleme identifizieren
: Schließen Sie den Drucker direkt an den Computer an. Konfigurieren Sie den Drucker zu Testzwecken als lokalen Drucker. Wenn dies funktioniert, werden die Probleme netzwerkseitig verursacht.

TCP/IP-Netzwerk prüfen
: Das TCP/IP-Netzwerk und die Namensauflösung müssen funktionieren.

Entfernten `lpd` prüfen
: Geben Sie den folgenden Befehl ein, um zu testen, ob zu `lpd` (Port `515`) auf *`host`* eine TCP-Verbindung hergestellt werden kann:

```
netcat -z host 515 && echo ok || echo failed
```

Wenn die Verbindung zu `lpd` nicht hergestellt werden kann, ist `lpd` entweder nicht aktiv oder es liegen grundlegende Netzwerkprobleme vor.

Geben Sie als `root` den folgenden Befehl ein, um einen (möglicherweise sehr langen) Statusbericht für *`queue`* auf dem entfernten *`host`* abzufragen, vorausgesetzt, der entsprechende `lpd` ist aktiv und der Host akzeptiert Abfragen:

```
echo -e "\004queue" \
| netcat -w 2 -p 722 host 515
```

Wenn `lpd` nicht antwortet, ist er entweder nicht aktiv oder es liegen grundlegende Netzwerkprobleme vor. Wenn `lpd` reagiert, sollte die Antwort zeigen, warum das Drucken in der `queue` auf `host` nicht möglich ist. Wenn Sie eine Antwort wie die in Beispiel 10.2, „Fehlermeldung von `lpd`“ (S. 137) erhalten, wird das Problem durch den entfernten `lpd` verursacht.

Beispiel 10.2 *Fehlermeldung von lpd*

```
lpd: your host does not have line printer access
lpd: queue does not exist
printer: spooling disabled
printer: printing disabled
```

Entfernten `cupsd` prüfen
: Standardmäßig sendet der CUPS-Netzwerkserver über Broadcast alle 30 Sekunden Informationen über seine Warteschlangen an UDP-Port `631`. Demzufolge kann

mit dem folgenden Befehl getestet werden, ob im Netzwerk ein CUPS-Netzwerkserver vorhanden ist. Stoppen Sie unbedingt Ihren lokalen CUPS-Daemon, bevor Sie das Kommando ausführen.

```
netcat -u -l -p 631 & PID=$! ; sleep 40 ; kill $PID
```

Wenn ein CUPS-Netzwerkserver vorhanden ist, der Informationen über Broadcasting sendet, erscheint die Ausgabe wie in Beispiel 10.3, „Broadcast vom CUPS-Netzwerkserver“ (S. 138) dargestellt.

Beispiel 10.3 *Broadcast vom CUPS-Netzwerkserver*

```
ipp://192.168.2.202:631/printers/queue
```

► **zseries:** Berücksichtigen Sie, dass IBM-System z-Ethernetgeräte standardmäßig keine Broadcasts empfangen. ◄

Mit dem folgenden Befehl können Sie testen, ob mit `cupsd` (Port `631`) auf *`host`* eine TCP-Verbindung hergestellt werden kann:

```
netcat -z host 631 && echo ok || echo failed
```

Wenn die Verbindung zu `cupsd` nicht hergestellt werden kann, ist `cupsd` entweder nicht aktiv oder es liegen grundlegende Netzwerkprobleme vor. `lpstat -h` *`host`* `-l -t` gibt einen (möglicherweise sehr langen) Statusbericht für alle Warteschlangen auf *`host`* zurück, vorausgesetzt, dass der entsprechende `cupsd` aktiv ist und der Host Abfragen akzeptiert.

Mit dem nächsten Befehl können Sie testen, ob die *`Warteschlange`* auf *`Host`* einen Druckauftrag akzeptiert, der aus einem einzigen CR-Zeichen (Carriage-Return) besteht. In diesem Fall sollte nichts gedruckt werden. Möglicherweise wird eine leere Seite ausgegeben.

```
echo -en "\r" \
| lp -d queue -h host
```

Fehlerbehebung für einen Netzwerkdrucker oder eine Print Server Box

Spooler, die in einer Print Server Box ausgeführt werden, verursachen gelegentlich Probleme, wenn sie viele Druckaufträge bearbeiten müssen. Da dies durch den Spooler in der Print Server Box verursacht wird, können Sie nichts dagegen tun. Sie haben jedoch die Möglichkeit, den Spooler in der Print Server-Box zu umgehen, indem Sie den an die Print Server-Box angeschlossenen Drucker über TCP-Socket

direkt ansprechen. Weitere Informationen hierzu finden Sie unter Abschnitt 10.4, „Netzwerkdrucker“ (S. 127).

Auf diese Weise wird die Print Server-Box auf einen Konvertierer zwischen den unterschiedlichen Formen der Datenübertragung (TCP/IP-Netzwerk und lokale Druckerverbindung) reduziert. Um diese Methode verwenden zu können, müssen Sie den TCP-Port der Print Server Box kennen. Wenn der Drucker eingeschaltet und an die Print Server Box angeschlossen ist, kann dieser TCP-Port in der Regel mit dem Dienstprogramm `nmap` aus dem Paket `nmap` ermittelt werden, wenn die Print Server Box einige Zeit eingeschaltet ist. Beispiel: `nmap` *`IP-Adresse`* gibt die folgende Ausgabe für eine Print Server-Box zurück:

```
Port       State       Service
23/tcp     open        telnet
80/tcp     open        http
515/tcp    open        printer
631/tcp    open        cups
9100/tcp   open        jetdirect
```

Diese Ausgabe gibt an, dass der an die Print Server-Box angeschlossene Drucker über TCP-Socket an Port `9100` angesprochen werden kann. `nmap` prüft standardmäßig nur eine bestimmte Anzahl der allgemein bekannten Ports, die in `/usr/share/nmap/nmap-services` aufgeführt sind. Um alle möglichen Ports zu überprüfen, verwenden Sie den Befehl `nmap -p` *`Ausgangs-Port-Ziel-PortIP-Adresse`*. Dies kann einige Zeit dauern. Weitere Informationen finden Sie auf der man-Seite zu `ypbind`.

Geben Sie einen Befehl ein wie

```
echo -en "\rHello\r\f" | netcat -w 1 IP-address port
cat file | netcat -w 1 IP-address port
```

um Zeichenketten oder Dateien direkt an den entsprechenden Port zu senden, um zu testen, ob der Drucker auf diesem Port angesprochen werden kann.

10.8.5 Fehlerhafte Ausdrucke ohne Fehlermeldung

Für das Drucksystem ist der Druckauftrag abgeschlossen, wenn das CUPS-Back-End die Datenübertragung an den Empfänger (Drucker) abgeschlossen hat. Wenn die weitere Verarbeitung auf dem Empfänger nicht erfolgt, z. B. wenn der Drucker die

druckerspezifischen Daten nicht drucken kann, wird dies vom Drucksystem nicht erkannt. Wenn der Drucker die druckerspezifischen Daten nicht drucken kann, wählen Sie eine andere PPD-Datei, die für den Drucker besser geeignet ist.

10.8.6 Deaktivierte Warteschlangen

Wenn die Datenübertragung zum Empfänger auch nach mehreren Versuchen nicht erfolgreich ist, meldet das CUPS-Back-End, z. B. `USB` oder `socket`, dem Drucksystem (an `cupsd`) einen Fehler. Das Backend entscheidet, ob und wie viele Versuche sinnvoll sind, bis die Datenübertragung als nicht möglich abgebrochen wird. Da weitere Versuche vergeblich wären, deaktiviert `cupsd` das Drucken für die entsprechende Warteschlange. Nachdem der Systemadministrator das Problem behoben hat, muss er das Drucken mit dem Kommando `cupsenable` wieder aktivieren.

10.8.7 CUPS-Browsing: Löschen von Druckaufträgen

Wenn ein CUPS-Netzwerkserver seine Warteschlangen den Client-Hosts via Browsing bekannt macht und auf den Host-Clients ein geeigneter lokaler `cupsd` aktiv ist, akzeptiert der Client-`cupsd` Druckaufträge von Anwendungen und leitet sie an den `cupsd` auf dem Server weiter. Wenn `cupsd` einen Druckauftrag akzeptiert, wird diesem eine neue Auftragsnummer zugewiesen. Daher unterscheidet sich die Auftragsnummer auf dem Client-Host von der auf dem Server. Da ein Druckauftrag in der Regel sofort weitergeleitet wird, kann er mit der Auftragsnummer auf dem Client-Host nicht gelöscht werden, da der Client- `cupsd` den Druckauftrag als abgeschlossen betrachtet, sobald dieser an den Server-`cupsd` weitergeleitet wurde.

Um einen Druckauftrag auf dem Server zu löschen, geben Sie ein Kommando wie `lpstat -h cups.example.com -o` ein. Sie ermitteln damit die Auftragsnummer auf dem Server, wenn der Server den Druckauftrag nicht bereits abgeschlossen (d. h. an den Drucker gesendet) hat. Mithilfe dieser Auftragsnummer kann der Druckauftrag auf dem Server gelöscht werden:

```
cancel -h cups.example.com queue-jobnnumber
```

10.8.8 Fehlerhafte Druckaufträge und Fehler bei der Datenübertragung

Druckaufträge verbleiben in den Warteschlangen und das Drucken wird fortgesetzt, wenn Sie den Drucker aus- und wieder einschalten oder den Computer während des Druckvorgangs herunterfahren und neu booten. Fehlerhafte Druckaufträge müssen mit `cancel` aus der Warteschlange entfernt werden.

Wenn ein Druckauftrag fehlerhaft ist oder während der Kommunikation zwischen dem Host und dem Drucker ein Fehler auftritt, druckt der Drucker mehrere Seiten Papier mit unleserlichen Zeichen, da er die Daten nicht ordnungsgemäß verarbeiten kann. Führen Sie die folgenden Schritte aus, um dies zu beheben:

1. Um den Druckvorgang zu beenden, entfernen Sie das Papier aus Tintenstrahldruckern oder öffnen Sie die Papierzufuhr bei Laserdruckern. Qualitativ hochwertige Drucker sind mit einer Taste zum Abbrechen des aktuellen Druckauftrags ausgestattet.

2. Der Druckauftrag befindet sich möglicherweise noch in der Warteschlange, da die Aufträge erst dann entfernt werden, wenn sie vollständig an den Drucker übertragen wurden. Geben Sie `lpstat -o` oder `lpstat -h cups.example.com -o` ein, um zu prüfen, über welche Warteschlange aktuell gedruckt wird. Löschen Sie den Druckauftrag mit `cancel` *`Warteschlange-Auftragsnummer`* oder mit `cancel -h cups.example.com` *`Warteschlange-Auftragsnummer`*.

3. Auch wenn der Druckauftrag aus der Warteschlange gelöscht wurde, werden einige Daten weiter an den Drucker gesendet. Prüfen Sie, ob ein CUPS-Backend-Prozess für die entsprechende Warteschlange ausgeführt wird und wenn ja, beenden Sie ihn. Für einen an den Parallelanschluss angeschlossenen Drucker geben Sie beispielsweise den Befehl `fuser -k /dev/lp0` ein, um alle Prozesse zu beenden, die aktuell noch auf den Drucker (den parallelen Port) zugreifen.

4. Setzen Sie den Drucker vollständig zurück, indem Sie ihn für einige Zeit ausschalten. Legen Sie anschließend Papier ein und schalten Sie den Drucker wieder ein.

10.8.9 Fehlerbehebung beim CUPS-Drucksystem

Suchen Sie Probleme im CUPS-Drucksystem mithilfe des folgenden generischen Verfahrens:

1. Setzen Sie `LogLevel debug` in `/etc/cups/cupsd.conf`.
2. Stoppen Sie `cupsd`.
3. Entfernen Sie `/var/log/cups/error_log*`, um das Durchsuchen sehr großer Protokolldateien zu vermeiden.
4. Starten Sie `cupsd`.
5. Wiederholen Sie die Aktion, die zu dem Problem geführt hat.
6. Lesen Sie die Meldungen in `/var/log/cups/error_log*`, um die Ursache des Problems zu identifizieren.

10.8.10 Weiterführende Informationen

Lösungen zu vielen spezifischen Problemen finden Sie in der Novell Knowledgebase (`http://support.novell.com/`). Die relevanten Themen finden Sie am schnellsten mittels einer Textsuche nach `CUPS`.

Gerätemanagemet über dynamischen Kernel mithilfe von udev

11

Der Kernel kann fast jedes Gerät am laufenden System hinzufügen oder entfernen. Änderungen des Gerätestatus (ob ein Gerät angeschlossen oder entfernt wird) müssen an den userspace weitergegeben werden. Geräte müssen konfiguriert werden, sobald sie angeschlossen und erkannt wurden. Benutzer eines bestimmten Geräts müssen über sämtliche Statusänderungen für das entsprechende Gerät informiert werden. udev bietet die erforderliche Infrastruktur, um die Geräteknotendateien und symbolische Links im `/dev`-Verzeichnis dynamisch zu warten. Mithilfe von udev-Regeln können externe Werkzeuge in die Ereignisverarbeitung des Kernel-Geräts eingebunden werden. Auf diese Weise können Sie die udev-Gerätebehandlung anpassen. Beispielsweise, indem Sie bestimmte Skripten hinzufügen, die als Teil der Kernel-Gerätebehandlung ausgeführt werden, oder indem Sie zusätzliche Daten zur Auswertung bei der Gerätebehandlung anfordern und importieren.

11.1 Das /dev-Verzeichnis

Die Geräteknoten im `/dev`-Verzeichnis ermöglichen den Zugriff auf die entsprechenden Kernel-Geräte. Mithilfe von udev spiegelt das `/dev`-Verzeichnis den aktuellen Status des Kernel wieder. Jedes Kernel-Gerät verfügt über eine entsprechende Gerätedatei. Falls ein Gerät vom System getrennt wird, wird der Geräteknoten entfernt.

Der Inhalt des `/dev`-Verzeichnisses wird auf einem temporären Dateisystem gespeichert und alle Dateien werden bei jedem Systemstart neu erstellt. Manuell erstellte oder geänderte Dateien überdauern ein erneutes Booten planmäßig nicht. Statische Dateien

und Verzeichnisse, die unabhängig vom Status des entsprechenden Kernel-Geräts immer im `/dev`-Verzeichnis vorhanden sein sollten, können im Verzeichnis `/lib/udev/devices` platziert werden. Beim Systemstart wird der Inhalt des entsprechenden Verzeichnisses in das `/dev`-Verzeichnis kopiert und erhält dieselbe Eigentümerschaft und dieselben Berechtigungen wie die Dateien in `/lib/udev/devices`.

11.2 Kernel-uevents und udev

Die erforderlichen Geräteinformationen werden vom sysfs-Dateisystem exportiert. Für jedes Gerät, das der Kernel erkannt und initialisiert hat, wird ein Verzeichnis mit dem Gerätenamen erstellt. Es enthält Attributdateien mit gerätespezifischen Eigenschaften.

Jedes Mal, wenn ein Gerät hinzugefügt oder entfernt wird, sendet der Kernel ein uevent, um udev über die Änderung zu informieren. Der udev-Daemon liest und analysiert alle angegebenen Regeln aus den `/etc/udev/rules.d/*.rules`-Dateien einmalig beim Start und speichert diese. Wenn Regeldateien geändert, hinzugefügt oder entfernt werden, kann der Daemon die Arbeitsspeicherrepräsentation aller Regeln mithilfe des Kommandos `udevadm control reload_rules` wieder laden. Dies ist auch beim Ausführen von `/etc/init.d/boot.udev reload` möglich. Weitere Informationen zu den udev-Regeln und deren Syntax finden Sie unter Abschnitt 11.6, „Einflussnahme auf das Gerätemanagemet über dynamischen Kernel mithilfe von udev-Regeln“ (S. 147).

Jedes empfangene Ereignis wird mit dem Satz der angegebenen Regeln abgeglichen. Die Regeln können Ereignisergebnisschlüssel hinzufügen oder ändern, einen bestimmten Namen für den zu erstellenden Geräteknoten anfordern, auf den Knoten verweisende Symlinks hinzufügen oder Programme hinzufügen, die ausgeführt werden sollen, nachdem der Geräteknoten erstellt wurde. Die Treiber-Core-uevents werden von einem Kernel-Netlink-Socket empfangen.

11.3 Treiber, Kernel-Module und Geräte

Die Kernel-Bus-Treiber prüfen, ob Geräte vorhanden sind. Für jedes erkannte Gerät erstellt der Kernel eine interne Gerätestruktur und der Treiber-Core sendet ein uevent

an den udev-Daemon. Bus-Geräte identifizieren sich mithilfe einer speziell formatierten ID, die Auskunft über die Art des Geräts gibt. Normalerweise bestehen diese IDs aus einer Hersteller- und einer Produkt-ID und anderen das Subsystem betreffenden Werten. Jeder Bus weist ein eigenes Schema für diese IDs auf, das so genannte `MODALIAS`-Schema. Der Kernel bedient sich der Geräteinformationen, verfasst daraus eine `MODALIAS`-ID-Zeichenkette und sendet diese Zeichenkette zusammen mit dem Ereignis. Beispiel für eine USB-Maus:

```
MODALIAS=usb:v046DpC03Ed2000dc00dsc00dp00ic03isc01ip02
```

Jeder Gerätetreiber verfügt über eine Liste bekannter Aliase für Geräte, die er behandeln kann. Die Liste ist in der Kernel-Moduldatei selbst enthalten. Das Programm depmod liest die ID-Listen und erstellt die Datei `modules.alias` im Verzeichnis `/lib/modules` des Kernel für alle zurzeit verfügbaren Module. Bei dieser Infrastruktur ist das Laden des Moduls ein ebenso müheloser Vorgang, wie das Aufrufen von `modprobe` für jedes Ereignis, das über einen `MODALIAS`-Schlüssel verfügt. Falls `modprobe $MODALIAS` aufgerufen wird, gleicht es den für das Gerät verfassten Geräte-Alias mit den Aliassen von den Modulen ab. Falls ein übereinstimmender Eintrag gefunden wird, wird das entsprechende Modul geladen. Alle diese Vorgänge werden von udev ausgelöst und erfolgen automatisch.

11.4 Booten und erstes Einrichten des Geräts

Alle Geräteereignisse, die während des Bootvorgangs stattfinden, bevor der udev-Daemon ausgeführt wird, gehen verloren. Dies liegt daran, dass die Infrastruktur für die Behandlung dieser Ereignisse sich auf dem Root-Dateisystem befindet und zu diesem Zeitpunkt nicht verfügbar ist. Diesen Verlust fängt der Kernel mit der Datei `uevent` ab, die sich im Geräteverzeichnis jedes Geräts im sysfs-Dateisystem befindet. Durch das Schreiben von `add` in die entsprechende Datei sendet der Kernel dasselbe Ereignis, das während des Bootvorgangs verloren gegangen ist, neu. Eine einfache Schleife über alle `uevent`-Dateien in `/sys` löst alle Ereignisse erneut aus, um die Geräteknoten zu erstellen und die Geräteeinrichtung durchzuführen.

Beispielsweise kann eine USB-Maus, die während des Bootvorgangs vorhanden ist, nicht durch die frühe Bootlogik initialisiert werden, da der Treiber zum entsprechenden Zeitpunkt nicht verfügbar ist. Das Ereignis für die Geräteerkennung ist verloren

gegangen und konnte kein Kernel-Modul für das Gerät finden. Anstatt manuell nach möglicherweise angeschlossenen Geräten zu suchen, fordert udev lediglich alle Geräteereignisse aus dem Kernel an, wenn das Root-Dateisystem verfügbar ist. Das Ereignis für die USB-Maus wird also lediglich erneut ausgeführt. Jetzt wird das Kernel-Modul auf dem eingehängten Root-Dateisystem gefunden und die USB-Maus kann initialisiert werden.

Von userspace aus gibt es keinen erkennbaren Unterschied zwischen einer coldplug-Gerätesequenz und einer Geräteerkennung während der Laufzeit. In beiden Fällen werden dieselben Regeln für den Abgleich verwendet und dieselben konfigurierten Programme ausgeführt.

11.5 Überwachen des aktiven udev-Daemons

Das Programm `udevadm monitor` kann verwendet werden, um die Treiber-Core-Ereignisse und das Timing der udev-Ereignisprozesse zu visualisieren.

```
UEVENT[1185238505.276660] add   /devices/pci0000:00/0000:00:1d.2/usb3/3-1
(usb)
UDEV  [1185238505.279198] add   /devices/pci0000:00/0000:00:1d.2/usb3/3-1
(usb)
UEVENT[1185238505.279527] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0 (usb)
UDEV  [1185238505.285573] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0 (usb)
UEVENT[1185238505.298878] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10 (input)
UDEV  [1185238505.305026] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10 (input)
UEVENT[1185238505.305442] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10/mouse2 (input)
UEVENT[1185238505.306440] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10/event4 (input)
UDEV  [1185238505.325384] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10/event4 (input)
UDEV  [1185238505.342257] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10/mouse2 (input)
```

Die `UEVENT`-Zeilen zeigen die Ereignisse an, die der Kernel an Netlink gesendet hat. Die `UDEV`-Zeilen zeigen die fertig gestellten udev-Ereignisbehandlungsroutinen an. Das Timing wird in Mikrosekunden angegeben. Die Zeit zwischen `UEVENT` und `UDEV` ist die Zeit, die udev benötigt hat, um dieses Ereignis zu verarbeiten oder der udev-

Daemon hat eine Verzögerung bei der Ausführung der Synchronisierung dieses Ereignisses mit zugehörigen und bereits ausgeführten Ereignissen erfahren. Beispielsweise warten Ereignisse für Festplattenpartitionen immer, bis das Ereignis für den primären Datenträger fertig gestellt ist, da die Partitionsereignisse möglicherweise auf die Daten angewiesen sind, die das Ereignis für den primären Datenträger von der Hardware angefordert hat.

`udevadm monitor --env` zeigt die vollständige Ereignisumgebung an:

```
ACTION=add
DEVPATH=/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10
SUBSYSTEM=input
SEQNUM=1181
NAME="Logitech USB-PS/2 Optical Mouse"
PHYS="usb-0000:00:1d.2-1/input0"
UNIQ=""
EV=7
KEY=70000 0 0 0 0
REL=103
MODALIAS=input:b0003v046DpC03Ee0110-e0,1,2,k110,111,112,r0,1,8,amlsfw
```

udev sendet auch Meldungen an syslog. Die Standard-syslog-Priorität, die steuert, welche Meldungen an syslog gesendet werden, wird in der udev-Konfigurationsdatei `/etc/udev/udev.conf` angegeben. Die Protokollpriorität des ausgeführten Daemons kann mit `udevadm control log_priority=`*`level/number`* geändert werden.

11.6 Einflussnahme auf das Gerätemanagemet über dynamischen Kernel mithilfe von udev-Regeln

Eine udev-Regel kann mit einer beliebigen Eigenschaft abgeglichen werden, die der Kernel der Ereignisliste hinzufügt oder mit beliebigen Informationen, die der Kernel in `sysfs` exportiert. Die Regel kann auch zusätzliche Informationen aus externen Programmen anfordern. Jedes Ereignis wird gegen alle angegebenen Regeln abgeglichen. Alle Regeln befinden sich im Verzeichnis `/etc/udev/rules.d/`.

Jede Zeile in der Regeldatei enthält mindestens ein Schlüsselwertepaar. Es gibt zwei Arten von Schlüsseln: die Übereinstimmungsschlüssel und Zuweisungsschlüssel. Wenn alle Übereinstimmungsschlüssel mit ihren Werten übereinstimmen, wird diese Regel angewendet und der angegebene Wert wird den Zuweisungsschlüsseln zugewiesen. Eine übereinstimmende Regel kann den Namen des Geräteknotens angeben, auf den Knoten verweisende Symlinks hinzufügen oder ein bestimmtes Programm als Teil der Ereignisbehandlung ausführen. Falls keine übereinstimmende Regel gefunden wird, wird der standardmäßige Geräteknotenname verwendet, um den Geräteknoten zu erstellen. Ausführliche Informationen zur Regelsyntax und den bereitgestellten Schlüsseln zum Abgleichen oder Importieren von Daten werden auf der man-Seite von udev beschrieben. Nachfolgend finden Sie einige Beispielregeln, die Sie in die grundlegende Regelsyntax von udev einführen. Sämtliche Beispielregeln stammen aus dem udev-Standardregelsatz, der sich in `/etc/udev/rules.d/50-udev-default.rules` befindet.

Beispiel 11.1 *udev-Beispielregeln*

```
# console
KERNEL=="console", MODE="0600", OPTIONS="last_rule"

# serial devices
KERNEL=="ttyUSB*", ATTRS{product}=="[Pp]alm*Handheld*", SYMLINK+="pilot"

# printer
SUBSYSTEM=="usb", KERNEL=="lp*", NAME="usb/%k", SYMLINK+="usb%k", GROUP="lp"

# kernel firmware loader
SUBSYSTEM=="firmware", ACTION=="add", RUN+="firmware.sh"
```

Die Regel `Konsole` besteht aus drei Schlüsseln: einem Übereinstimmungsschlüssel (`KERNEL`) und zwei Zuordnungsschlüsseln (`MODE`, `OPTIONS`). Der Übereinstimmungsschlüssel `KERNEL` durchsucht die Geräteliste nach Elementen des Typs `console`. Nur exakte Übereinstimmungen sind gültig und lösen die Ausführung dieser Regel aus. Der Zuweisungsschlüssel `MODE` weist dem Geräteknoten spezielle Berechtigungen zu, in diesem Fall Lese- und Schreibberechtigung nur für den Eigentümer des Geräts. Der Schlüssel `OPTIONS` bewirkt, dass diese Regel auf Geräte dieses Typs als letzte Regel angewendet wird. Alle nachfolgenden Regeln, die mit diesem Gerätetyp übereinstimmen, werden nicht mehr angewendet.

Die Regel `Serielle Geräte` steht in `50-udev-default.rules` nicht mehr zur Verfügung; es lohnt sich jedoch, sie sich dennoch anzusehen. Sie besteht aus zwei Übereinstimmungsschlüsseln (`KERNEL` und `ATTRS`) und einem Zuweisungsschlüssel

(SYMLINK). Der Übereinstimmungsschlüssel KERNEL sucht nach allen Geräten des Typs ttyUSB. Durch den Platzhalter * trifft dieser Schlüssel auf mehrere dieser Geräte zu. Der zweite Übereinstimmungsschlüssel (ATTRS) überprüft, ob die Attributdatei product in sysfs der jeweiligen ttyUSB-Geräte eine bestimmte Zeichenkette enthält. Der Zuweisungsschlüssel SYMLINK bewirkt, dass dem Gerät unter /dev/pilot ein symbolischer Link hinzugefügt wird. Der Operator dieses Schlüssels (+=) weist udev an, diese Aktion auch dann auszuführen, wenn dem Gerät bereits durch frühere (oder auch erst durch spätere) Regeln andere symbolische Links hinzugefügt wurden. Die Regel wird nur angewendet, wenn die Bedingungen beider Übereinstimmungsschlüssel erfüllt sind.

Die Regel printer gilt nur für USB-Drucker. Sie enthält zwei Übereinstimmungsschlüssel (SUBSYSTEM und KERNEL), die beide zutreffen müssen, damit die Regel angewendet wird. Die drei Zuweisungsschlüssel legen den Namen dieses Gerätetyps fest (NAME), die Erstellung symbolischer Gerätelinks (SYMLINK) sowie die Gruppenmitgliedschaft dieses Gerätetyps (GROUP). Durch den Platzhalter * im Schlüssel KERNEL trifft diese Regel auf mehrere lp-Druckergeräte zu. Sowohl der Schlüssel NAME als auch der Schlüssel SYMLINK verwenden Ersetzungen, durch die der Zeichenkette der interne Gerätename hinzugefügt wird. Der symbolische Link für den ersten lp-USB-Drucker würde zum Beispiel /dev/usblp0 lauten.

Die Regel kernel firmware loader weist udev an, während der Laufzeit weitere Firmware mittels eines externen Hilfsskripts zu laden. Der Übereinstimmungsschlüssel SUBSYSTEM sucht nach dem Subsystem firmware. Der Schlüssel ACTION überprüft, ob bereits Geräte des Subsystems firmware hinzugefügt wurden. Der Schlüssel RUN+= löst die Ausführung des Skripts firmware.sh aus, das die noch zu ladende Firmware lokalisiert.

Die folgenden allgemeinen Eigenschaften treffen auf alle Regeln zu:

- Jede Regel besteht aus einem oder mehreren, durch Kommas getrennten Schlüssel-/Wertepaaren.
- Die Aktion eines Schlüssels wird durch seinen Operator festgelegt. udev-Regeln unterstützen verschiedene Operatoren.
- Jeder angegebene Wert muss in Anführungszeichen eingeschlossen sein.

- Jede Zeile der Regeldatei stellt eine Regel dar. Falls eine Regel länger als eine Zeile ist, verbinden Sie die Zeilen wie bei jeder anderen Shell-Syntax mit `\`.
- udev-Regeln unterstützen Shell-typische Übereinstimmungsregeln für die Schemata `*`, `?` und `[]`.
- udev-Regeln unterstützen Ersetzungen.

11.6.1 Verwenden von Operatoren in udev-Regeln

Bei der Erstellung von Schlüsseln stehen Ihnen je nach gewünschtem Schlüsseltyp verschiedene Operatoren zur Auswahl. Übereinstimmungsschlüssel werden in der Regel nur zum Auffinden eines Wertes verwendet, der entweder mit dem Suchwert übereinstimmt oder explizit nicht mit dem gesuchten Wert übereinstimmt. Übereinstimmungsschlüssel enthalten einen der folgenden Operatoren:

`==`
: Suche nach übereinstimmendem Wert. Wenn der Schlüssel ein Suchschema enthält, sind alle Ergebnisse gültig, die mit diesem Schema übereinstimmen.

`!=`
: Suche nach nicht übereinstimmendem Wert. Wenn der Schlüssel ein Suchschema enthält, sind alle Ergebnisse gültig, die mit diesem Schema übereinstimmen.

Folgende Operatoren können für Zuweisungsschlüssel verwendet werden:

`=`
: Weist einem Schlüssel einen Wert zu. Wenn der Schlüssel zuvor aus einer Liste mit mehreren Werten bestand, wird der Schlüssel durch diesen Operator auf diesen Einzelwert zurückgesetzt.

`+=`
: Fügt einem Schlüssel, der eine Liste mehrerer Einträge enthält, einen Wert hinzu.

`:=`
: Weist einen endgültigen Wert zu. Eine spätere Änderung durch nachfolgende Regeln ist nicht möglich.

11.6.2 Verwenden von Ersetzungen in udev-Regeln

udev-Regeln unterstützen sowohl Platzhalter als auch Ersetzungen. Diese setzen Sie genauso ein wie in anderen Skripten. Folgende Ersetzungen können in udev-Regeln verwendet werden:

`%r`, `$root`
: Standardmäßig das Geräteverzeichnis `/dev`.

`%p`, `$devpath`
: Der Wert von `DEVPATH`.

`%k`, `$kernel`
: Der Wert von `KERNEL` oder der interne Gerätename.

`%n`, `$number`
: Die Gerätenummer.

`%N`, `$tempnode`
: Der temporäre Name der Gerätedatei.

`%M`, `$major`
: Die höchste Nummer des Geräts.

`%m`, `$minor`
: Die niedrigste Nummer des Geräts.

`%s{`*`attribute`*`}`, `$attr{`*`attribute`*`}`
: Der Wert eines `sysfs`-Attributs (das durch *`attribute`* festgelegt ist).

`%E{`*`variable`*`}`, `$attr{`*`variable`*`}`
: Der Wert einer Umgebungsvariablen (die durch *`variable`* festgelegt ist).

`%c`, `$result`
: Die Ausgabe von `PROGRAM`.

`%%`
: Das `%`-Zeichen.

`$$`
: Das `$`-Zeichen.

11.6.3 Verwenden von udev-Übereinstimmungsschlüsseln

Übereinstimmungsschlüssel legen Bedingungen fest, die erfüllt sein müssen, damit eine udev-Regel angewendet werden kann. Folgende Übereinstimmungsschlüssel sind verfügbar:

`ACTION`
: Der Name der Ereignisaktion, z. B. `add` oder `remove` beim Hinzufügen oder Entfernen eines Geräts.

`DEVPATH`
: Der Gerätepfad des Ereignisgeräts, zum Beispiel `DEVPATH=/bus/pci/drivers/ipw3945` für die Suche nach allen Ereignissen in Zusammenhang mit dem Treiber ipw3945.

`KERNEL`
: Der interne Name (Kernel-Name) des Ereignisgeräts.

`SUBSYSTEM`
: Das Subsystem des Ereignisgeräts, zum Beispiel `SUBSYSTEM=usb` für alle Ereignisse in Zusammenhang mit USB-Geräten.

`ATTR{`*`Dateiname`*`}`
: sysfs-Attribute des Ereignisgeräts. Für die Suche nach einer Zeichenkette im Attributdateinamen `vendor` können Sie beispielsweise `ATTR{vendor}=="On[sS]tream"` verwenden.

`KERNELS`
: Weist udev an, den Gerätepfad aufwärts nach einem übereinstimmenden Gerätenamen zu durchsuchen.

SUBSYSTEMS
: Weist udev an, den Gerätepfad aufwärts nach einem übereinstimmenden Geräte-Subsystemnamen zu durchsuchen.

DRIVERS
: Weist udev an, den Gerätepfad aufwärts nach einem übereinstimmenden Gerätetreibernamen zu durchsuchen.

ATTRS{*Dateiname*}
: Weist udev an, den Gerätepfad aufwärts nach einem Gerät mit übereinstimmenden sysfs-Attributwerten zu durchsuchen.

ENV{*Schlüssel*}
: Der Wert einer Umgebungsvariablen, zum Beispiel `ENV{ID_BUS}="ieee1394` für die Suche nach allen Ereignissen in Zusammenhang mit der FireWire-Bus-ID.

PROGRAM
: Weist udev an, ein externes Programm auszuführen. Damit es erfolgreich ist, muss das Programm mit Beendigungscode Null abschließen. Die Programmausgabe wird in stdout geschrieben und steht dem Schlüssel `RESULT` zur Verfügung.

RESULT
: Überprüft die Rückgabezeichenkette des letzten `PROGRAM`-Aufrufs. Diesen Schlüssel können Sie entweder sofort der Regel mit dem `PROGRAM`-Schlüssel hinzufügen oder erst einer nachfolgenden Regel.

11.6.4 Verwenden von udev-Zuweisungsschlüsseln

Im Gegensatz zu den zuvor beschriebenen Übereinstimmungsschlüsseln definieren Zuweisungsschlüssel keine Bedingungen, die erfüllt sein müssen, sondern sie weisen den von udev verwalteten Geräteknoten Werte, Namen und Aktionen zu.

NAME
: Der Name des zu erstellenden Geräteknotens. Nachdem der Knotenname durch eine Regel festgelegt wurde, werden alle anderen Regeln mit dem Schlüssel `NAME`, die auf diesen Knoten zutreffen, ignoriert.

`SYMLINK`
: Der Name eines symbolischen Links, der dem zu erstellenden Knoten hinzugefügt werden soll. Einem Geräteknoten können mittels mehrerer Zuweisungsregeln mehrere symbolische Links hinzugefügt werden. Ebenso können Sie aber mehrere symbolische Links für einen Knoten auch in einer Regel angeben. Die Namen der einzelnen Symlinks müssen in diesem Fall jeweils durch ein Leerzeichen getrennt sein.

`OWNER, GROUP, MODE`
: Die Berechtigungen für den neuen Geräteknoten. Die hier angegebenen Werte überschreiben sämtliche kompilierten Werte.

`ATTR{`*`Schlüssel`*`}`
: Gibt einen Wert an, der in ein sysfs-Attribut des Ereignisgeräts geschrieben werden soll. Wenn der Operator == verwendet wird, überprüft dieser Schlüssel, ob der Wert eines sysfs-Attributs mit dem angegebenen Wert übereinstimmt.

`ENV{`*`Schlüssel`*`}`
: Weist udev an, eine Umgebungsvariable zu exportieren. Wenn der Operator == verwendet wird, überprüft dieser Schlüssel, ob der Wert einer Umgebungsvariable mit dem angegebenen Wert übereinstimmt.

`RUN`
: Weist udev an, der Liste der für dieses Gerät auszuführenden Programme ein Programm hinzuzufügen. Sie sollten hier nur sehr kurze Aufgaben angeben. Anderenfalls laufen Sie Gefahr, dass weitere Ereignisse für dieses Gerät blockiert werden.

`LABEL`
: Fügt der Regel eine Bezeichnung hinzu, zu der ein `GOTO` direkt wechseln kann.

`GOTO`
: Weist udev an, eine Reihe von Regeln auszulassen und direkt mit der Regel fortzufahren, die die von `GOTO` angegebene Bezeichnung enthält.

`IMPORT{`*`Typ`*`}`
: Lädt Variablen in die Ereignisumgebung, beispielsweise die Ausgabe eines externen Programms. udev kann verschiedene Variablentypen importieren. Wenn kein Typ angegeben ist, versucht udev den Typ anhand des ausführbaren Teils der Dateiberechtigungen selbst zu ermitteln.

- `program` weist udev an, ein externes Programm auszuführen und dessen Ausgabe zu importieren.
- `file` weist udev an, eine Textdatei zu importieren.
- `parent` weist udev an, die gespeicherten Schlüssel des übergeordneten Geräts zu importieren.

`WAIT_FOR_SYSFS`
: Weist udev an, auf die Erstellung der angegebenen sysfs-Datei für ein bestimmtes Gerät zu warten. Beispiel: `WAIT_FOR_SYSFS="ioerr_cnt"` fordert udev auf, so lange zu warten, bis die Datei `ioerr_cnt` erstellt wurde.

`OPTIONEN`
: Der Schlüssel `OPTION` kann mehrere mögliche Werte haben:

- `last_rule` weist udev an, alle nachfolgenden Regeln zu ignorieren.
- `ignore_device` weist udev an, dieses Ereignis komplett zu ignorieren.
- `ignore_remove` weist udev an, alle späteren Entfernungsereignisse für dieses Gerät zu ignorieren.
- `all_partitions` weist udev an, für alle vorhandenen Partitionen eines Blockgeräts Geräteknoten zu erstellen.

11.7 Permanente Gerätebenennung

Das dynamische Geräteverzeichnis und die Infrastruktur für die udev-Regeln ermöglichen die Bereitstellung von stabilen Namen für alle Laufwerke unabhängig von ihrer Erkennungsreihenfolge oder der für das Gerät verwendeten Verbindung. Jedes geeignete Blockgerät, das der Kernel erstellt, wird von Werkzeugen mit speziellen Kenntnissen über bestimmte Busse, Laufwerktypen oder Dateisysteme untersucht. Gemeinsam mit dem vom dynamischen Kernel bereitgestellten Geräteknotennamen unterhält udev Klassen permanenter symbolischer Links, die auf das Gerät verweisen:

```
/dev/disk
|-- by-id
|   |-- scsi-SATA_HTS726060M9AT00_MRH453M4HWHG7B -> ../../sda
|   |-- scsi-SATA_HTS726060M9AT00_MRH453M4HWHG7B-part1 -> ../../sda1
```

```
|   |-- scsi-SATA_HTS726060M9AT00_MRH453M4HWHG7B-part6 -> ../../sda6
|   |-- scsi-SATA_HTS726060M9AT00_MRH453M4HWHG7B-part7 -> ../../sda7
|   |-- usb-Generic_STORAGE_DEVICE_02773 -> ../../sdd
|   `-- usb-Generic_STORAGE_DEVICE_02773-part1 -> ../../sdd1
|-- by-label
|   |-- Photos -> ../../sdd1
|   |-- SUSE10 -> ../../sda7
|   `-- devel -> ../../sda6
|-- by-path
|   |-- pci-0000:00:1f.2-scsi-0:0:0:0 -> ../../sda
|   |-- pci-0000:00:1f.2-scsi-0:0:0:0-part1 -> ../../sda1
|   |-- pci-0000:00:1f.2-scsi-0:0:0:0-part6 -> ../../sda6
|   |-- pci-0000:00:1f.2-scsi-0:0:0:0-part7 -> ../../sda7
|   |-- pci-0000:00:1f.2-scsi-1:0:0:0 -> ../../sr0
|   |-- usb-02773:0:0:2 -> ../../sdd
|   |-- usb-02773:0:0:2-part1 -> ../../sdd1
`-- by-uuid
    |-- 159a47a4-e6e6-40be-a757-a629991479ae -> ../../sda7
    |-- 3e999973-00c9-4917-9442-b7633bd95b9e -> ../../sda6
    `-- 4210-8F8C -> ../../sdd1
```

11.8 Von udev verwendete Dateien

`/sys/*`
: Virtuelles, vom Linux-Kernel bereitgestelltes Dateisystem, das alle zur Zeit bekannten Geräte exportiert. Diese Informationen werden von udev zur Erstellung von Geräteknoten in `/dev` verwendet.

`/dev/*`
: Dynamisch erstellte Geräteknoten und statische Inhalte, die beim Booten aus `/lib/udev/devices/*` kopiert werden.

Die folgenden Dateien und Verzeichnisse enthalten die entscheidenden Elemente der udev-Infrastruktur:

`/etc/udev/udev.conf`
: Wichtigste udev-Konfigurationsdatei.

`/etc/udev/rules.d/*`
: udev-Ereigniszuordnungsregeln.

`/lib/udev/devices/*`
: Statischer `/dev`-Inhalt.

`/lib/udev/*`
: Von den udev-Regeln aufgerufene Helferprogramme.

11.9 Weiterführende Informationen

Weitere Informationen zur udev-Infrastruktur finden Sie auf den folgenden Manualpages:

udev
: Allgemeine Informationen zu udev, Schlüssel, Regeln und anderen wichtigen Konfigurationsbelangen.

udevadm
: udevadm kann dazu verwendet werden, das Laufzeitverhalten von udev zu kontrollieren, Kernel-Ereignisse abzurufen, die Ereigniswarteschlange zu verwalten und einfache Methoden zur Fehlersuche bereitzustellen.

udevd
: Informationen zum udev-Ereignisverwaltungs-Daemon.

12 Das X Window-System

Das X Window-System (X11) ist der Industriestandard für grafische Bedienoberflächen unter UNIX. X ist netzwerkbasiert und ermöglicht es, auf einem Host gestartete Anwendungen auf einem anderen, über eine beliebige Art von Netzwerk (LAN oder Internet) verbundenen Host anzuzeigen. In diesem Kapitel werden die Einrichtung und die Optimierung der X Window-Systemumgebung beschrieben. Sie erhalten dabei Hintergrundinformationen zur Verwendung von Schriften in SUSE® Linux Enterprise Server.

TIPP: IBM-System z: Konfigurieren der grafischen Bedienoberfläche

IBM-System z verfügen über keine von X.Org unterstützten Eingabe- oder Ausgabegeräte Daher treffen keine der in diesem Abschnitt beschriebenen Konfigurationsverfahren zu. Weitere relevante Informationen für IBM-System z finden Sie in Kapitel 4, *Installation auf IBM System z* (↑*Bereitstellungshandbuch*).

12.1 Manuelles Konfigurieren des X Window-Systems

Standardmäßig ist das X Window System mit der unter Abschnitt „Einrichten von Grafikkarte und Monitor“ (Kapitel 8, *Einrichten von Hardware-Komponenten mit YaST*, ↑*Bereitstellungshandbuch*) beschriebenen SaX2-Schnittstelle konfiguriert. Alternativ kann es manuell konfiguriert werden, indem Sie die Konfigurationsdateien bearbeiten.

WARNUNG: Fehlerhafte X-Konfigurationen können Ihre Hardware beschädigen

Seien Sie sehr vorsichtig, wenn Sie die Konfiguration des X Window-Systems ändern. Starten Sie auf keinen Fall das X Window-System, bevor die Konfiguration abgeschlossen ist. Ein falsch konfiguriertes System kann Ihre Hardware irreparabel beschädigen (dies gilt insbesondere für Monitore mit fester Frequenz). Die Autoren dieses Buchs und die Entwickler von SUSE Linux Enterprise Server übernehmen keine Haftung für mögliche Schäden. Die folgenden Informationen basieren auf sorgfältiger Recherche. Es kann jedoch nicht garantiert werden, dass alle hier aufgeführten Methoden fehlerfrei sind und keinen Schaden an Ihrer Hardware verursachen können.

Das Kommando `sax2` erstellt die Datei `/etc/X11/xorg.conf`. Dabei handelt es sich um die primäre Konfigurationsdatei des X Window System. Hier finden Sie alle Einstellungen, die Grafikkarte, Maus und Monitor betreffen.

WICHTIG: Verwenden von X -configure

Verwenden Sie `X -configure` zur Konfiguration Ihres X-Setups, wenn vorherige Versuche mit SaX2 von SUSE Linux Enterprise Server nicht erfolgreich waren. Wenn Ihr Setup ausschließlich proprietäre Binärtreiber umfasst, funktioniert `X -configure` nicht.

In den folgenden Abschnitten wird die Struktur der Konfigurationsdatei `/etc/X11/xorg.conf` beschrieben. Sie ist in mehrere Abschnitte gegliedert, die jeweils für bestimmte Aspekte der Konfiguration verantwortlich sind. Jeder Abschnitt beginnt mit dem Schlüsselwort `Section <Bezeichnung>` und endet mit `EndSection`. Die folgende Konvention gilt für alle Abschnitte:

```
Section "designation"
  entry 1
  entry 2
  entry n
EndSection
```

Die verfügbaren Abschnittstypen finden Sie in Tabelle 12.1, „Abschnitte in /etc/X11/xorg.conf“ (S. 161).

Tabelle 12.1 *Abschnitte in /etc/X11/xorg.conf*

Typ	Bedeutung
`Dateien`	Die Pfade für die Schriften und die RGB-Farbtabelle.
`ServerFlags`	Allgemeine Schalter für das Serververhalten.
`Modul`	Eine Liste mit Modulen, die der Server laden sollte
`InputDevice`	Eingabegeräte wie Tastaturen und spezielle Eingabegeräte (Touchpads, Joysticks usw.) werden in diesem Abschnitt konfiguriert. Wichtige Parameter in diesem Abschnitt sind `Driver` und die Optionen für `Protocol` und `Device`. Normalerweise ist dem Computer ein `InputDevice`-Abschnitt pro Gerät angefügt.
`Monitor`	Der verwendete Monitor. Wichtige Elemente dieses Abschnitts sind die Kennung (`Identifier`), auf die später in der Definition von `Screen` eingegangen wird, die Aktualisierungsrate (`VertRefresh`) und die Grenzwerte für die Synchronisierungsfrequenz (`HorizSync` und `VertRefresh`). Die Einstellungen sind in MHz, kHz und Hz angegeben. Normalerweise akzeptiert der Server nur Modeline-Werte, die den Spezifikationen des Monitors entsprechen. Dies verhindert, dass der Monitor versehentlich mit zu hohen Frequenzen angesteuert wird.
`Modi`	Die Modeline-Parameter für die spezifischen Bildschirmauflösungen. Diese Parameter können von SaX2 auf Grundlage der vom Benutzer vorgegebenen Werte berechnet werden und müssen in der Regel nicht geändert werden. Nehmen Sie hier beispielsweise dann Änderungen vor, wenn Sie einen Monitor mit fester Frequenz anschließen möchten. Details zur Bedeutung der einzelnen Zahlenwerte finden Sie in den HOWTO-Dateien unter `/usr/share/doc/howto/en/html/XFree86-Video-Timings-HOWTO` (im Paket `howtoenh`). Zur manuellen Berechnung von VESA-Modi können Sie das Tool `cvt` verwenden. Verwenden Sie z. B. zur Berechnung

Typ	Bedeutung
	einer Modeline für einen 1680x1050@60Hz-Monitor das Kommando `cvt 1680 1050 60`.
`Gerät`	Eine spezifische Grafikkarte. Sie wird mit ihrem beschreibenden Namen angeführt. Die in diesem Abschnitt verfügbaren Optionen hängen stark vom verwendeten Treiber ab. Wenn Sie beispielsweise den `i810`-Treiber verwenden, erhalten Sie weitere Informationen auf der man-Seite `man 4 i810`.
`Screen`	Verbindet einen `Monitor` und ein `Device` , damit alle erforderlichen Einstellungen für X.Org gewährleistet sind. Geben Sie im Unterabschnitt `Display` die Größe des virtuellen Bildschirms (`Virtual`), den `ViewPort` und die für diesen Bildschirm verwendeten Modi (`Modes`) an. Beachten Sie, dass einige Treiber es erfordern, dass alle verwendeten Konfigurationen an einer Stelle im Abschnitt `Display` vorhanden sein müssen. Wenn Sie beispielsweise an einem Laptop einen externen Monitor verwenden möchten, der größer als das interne LCD-Display ist, kann es erforderlich sein, eine höhere Auflösung als die vom internen LCD-Display unterstützte an das Ende der Zeile `Modes` anzufügen.
`ServerLayout`	Das Layout einer Einzel- oder Multihead-Konfiguration. In diesem Abschnitt werden Kombinationen aus Eingabegeräten (`InputDevice`) und Anzeigegeräten (`Screen`) festgelegt.
`DRI`	Bietet Informationen für die Direct Rendering Infrastructure (DRI).

`Monitor`, `Device` und `Screen` werden im Folgenden genauer erläutert. Weitere Informationen zu den anderen Abschnitten finden Sie auf den man-Seiten von `X.Org` und `xorg.conf`.

Die Datei `xorg.conf` kann mehrere unterschiedliche Abschnitte vom Typ `Monitor` und `Device` enthalten. Manchmal gibt es sogar mehrere Abschnitte vom Typ `Screen`. Der Abschnitt `ServerLayout` legt fest, welche dieser Abschnitte verwendet werden.

12.1.1 Abschnitt "Screen"

Der Abschnitt "Screen" kombiniert einen Monitor mit einem Device-Abschnitt und legt fest, welche Auflösung und Farbtiefe verwendet werden sollen. Der Abschnitt "Screen" kann beispielsweise wie in Beispiel 12.1, „Abschnitt "Screen" der Datei /etc/X11/xorg.conf“ (S. 163) aussehen.

Beispiel 12.1 *Abschnitt "Screen" der Datei /etc/X11/xorg.conf*

```
Section "Screen"❶
  DefaultDepth  16❷
  SubSection "Display"❸
    Depth       16❹
    Modes       "1152x864" "1024x768" "800x600"❺
    Virtual     1152x864❻
  EndSubSection
  SubSection "Display"
    Depth       24
    Modes       "1280x1024"
  EndSubSection
  SubSection "Display"
    Depth       32
    Modes "640x480"
  EndSubSection
  SubSection "Display"
    Depth        8
    Modes       "1280x1024"
  EndSubSection
  Device        "Device[0]"
  Identifier    "Screen[0]"❼
  Monitor       "Monitor[0]"
EndSection
```

❶ `Section` legt den Typ des Abschnitts fest, in diesem Fall `Screen`.

❷ `DefaultDepth` bestimmt die Farbtiefe, die standardmäßig verwendet werden soll, wenn keine andere Farbtiefe explizit angegeben wird.

❸ Für jede Farbtiefe werden verschiedene `Display`-Unterabschnitte angegeben.

❹ `Depth` bestimmt die Farbtiefe, die mit diesem Satz von `Display`-Einstellungen benutzt werden soll. Mögliche Werte sind `8`, `15`, `16`, `24` und `32`, obwohl mögli-

cherweise nicht alle davon durch alle X-Server-Module oder -Auflösungen unterstützt werden.

❺ Der Abschnitt `Modes` enthält eine Liste der möglichen Bildschirmauflösungen. Diese Liste wird vom X-Server von links nach rechts gelesen. Zu jeder Auflösung sucht der X-Server eine passende `Modeline` im Abschnitt `Modes`. Die `Modeline` ist von den Fähigkeiten des Monitors und der Grafikkarte abhängig. Die Einstellungen unter `Monitor` bestimmen die `Modeline`.

Die erste passende Auflösung ist der Standardmodus (`Default mode`). Mit Strg + Alt + + + (auf dem Ziffernblock) können Sie zur nächsten Auflösung rechts in der Liste wechseln. Mit Strg + Alt + – (auf dem Ziffernblock) können Sie zur vorherigen Auflösung wechseln. So lässt sich die Auflösung ändern, während X ausgeführt wird.

❻ Die letzte Zeile des Unterabschnitts `Display` mit `Depth 16` bezieht sich auf die Größe des virtuellen Bildschirms. Die maximal mögliche Größe eines virtuellen Bildschirms ist von der Menge des Arbeitsspeichers auf der Grafikkarte und der gewünschten Farbtiefe abhängig, nicht jedoch von der maximalen Auflösung des Monitors. Wenn Sie diese Zeile auslassen, entspricht die virtuelle Auflösung der physikalischen Auflösung. Da moderne Grafikkarten über viel Grafikspeicher verfügen, können Sie sehr große virtuelle Desktops erstellen. Gegebenenfalls ist es aber nicht mehr möglich, 3-D-Funktionen zu nutzen, wenn ein virtueller Desktop den größten Teil des Grafikspeichers belegt. Wenn die Grafikkarte beispielsweise über 16 MB RAM verfügt, kann der virtuelle Bildschirm bei einer Farbtiefe von 8 Bit bis zu 4096 x 4096 Pixel groß sein. Insbesondere bei beschleunigten Grafikkarten ist es nicht empfehlenswert, den gesamten Arbeitsspeicher für den virtuellen Bildschirm zu verwenden, weil der Kartenspeicher auch für diverse Schrift- und Grafik-Caches genutzt wird.

❼ In der Zeile `Identifier` (hier `Screen[0]`) wird für diesen Abschnitt ein Name vergeben, der als eindeutige Referenz im darauf folgenden Abschnitt `ServerLayout` verwendet werden kann. Die Zeilen `Device` und `Monitor` geben die Grafikkarte und den Monitor an, die zu dieser Definition gehören. Hierbei handelt es sich nur um Verbindungen zu den Abschnitten `Device` und `Monitor` mit ihren entsprechenden Namen bzw. Kennungen (*identifiers*). Diese Abschnitte werden weiter unten detailliert beschrieben.

12.1.2 Abschnitt "Device"

Im Abschnitt "Device" wird eine bestimmte Grafikkarte beschrieben. `xorg.conf` kann beliebig viele Grafikkarteneinträge enthalten. Jedoch muss der Name der Grafikkarten eindeutig sein. Hierfür wird das Schlüsselwort `Identifier` verwendet. Wenn mehrere Grafikkarten installiert sind, werden die Abschnitte einfach der Reihe nach nummeriert. Die erste wird als `Device[0]`, die zweite als `Device[1]` usw. eingetragen. Die folgende Datei zeigt einen Auszug aus dem Abschnitt `Device` eines Computers mit einer Matrox Millennium PCI-Grafikkarte (wie von SaX2 konfiguriert):

```
Section "Device"
  BoardName     "MGA2064W"
  BusID         "0:19:0"❶
  Driver        "mga"❷
  Identifier    "Device[0]"
  VendorName    "Matrox"
  Option        "sw_cursor"
EndSection
```

❶ Der Wert unter `BusID` steht für den PCI- oder AGP-Steckplatz, in dem die Grafikkarte installiert ist. Er entspricht der ID, die bei Eingabe des Befehls `lspci` angezeigt wird. Der X-Server benötigt Informationen im Dezimalformat, `lspci` zeigt die Informationen jedoch im Hexadezimalformat an. Der Wert von `BusID` wird von SaX2 automatisch erkannt.

❷ Der Wert von `Driver` wird automatisch von SaX2 eingestellt und gibt den Treiber an, der für Ihre Grafikkarte verwendet wird. Wenn es sich um eine Matrox Millennium-Grafikkarte handelt, heißt das Treibermodul `mga`. Anschließend durchsucht der X-Server den `ModulePath`, der im Abschnitt `Files` des Unterverzeichnisses `drivers` angegeben ist. In einer Standardinstallation ist dies das Verzeichnis `/usr/lib/xorg/modules/drivers` oder das Verzeichnis `/usr/lib64/xorg/modules/drivers` für 64-Bit-Betriebssysteme. `_drv.o` wird an den Namen angehängt, sodass beispielsweise im Falle des `mga`-Treibers die Treiberdatei `mga_drv.o` geladen wird.

Das Verhalten des X-Servers bzw. des Treibers kann außerdem durch weitere Optionen beeinflusst werden. Ein Beispiel hierfür ist die Option `sw_cursor`, die im Abschnitt "Device" festgelegt wird. Diese deaktiviert den Hardware-Mauszeiger und stellt den Mauszeiger mithilfe von Software dar. Je nach Treibermodul können verschiedene Optionen verfügbar sein. Diese finden Sie in den Beschreibungsdateien der Treibermodule im Verzeichnis `/usr/share/doc/`*`paket_name`*. Allgemeingültige Optionen

finden Sie außerdem auf den entsprechenden man-Seiten (`man xorg.conf`, `man 4 <Treibermodul>` und `man 4 chips`).

Wenn die Grafikkarte über mehrere Videoanschlüsse verfügt, können die verschiedenen an der Karte angeschlossenen Geräte in SaX2 als eine Ansicht konfiguriert werden.

12.1.3 Abschnitte "Monitor" und "Modes"

So wie die Abschnitte vom Typ `Device` jeweils für eine Grafikkarte verwendet werden, beschreiben die Abschnitte `Monitor` und `Modes` jeweils einen Monitor. Die Konfigurationsdatei `/etc/X11/xorg.conf` kann beliebig viele Abschnitte vom Typ `Monitor` enthalten. Jeder `Monitor`-Abschnitt verweist, sofern verfügbar, auf einen `Modes`-Abschnitt mit der Zeile `UseModes`. Wenn für den Abschnitt `Monitor` kein `Modes`-Abschnitt zur Verfügung steht, berechnet der X-Server aus den allgemeinen Synchronisierungswerten passende Werte. Der Abschnitt "ServerLayout" gibt an, welcher `Monitor`-Abschnitt zu verwenden ist.

Monitordefinitionen sollten nur von erfahrenen Benutzern festgelegt werden. Die Modelines stellen einen bedeutenden Teil der `Monitor`-Abschnitte dar. Modelines legen die horizontalen und vertikalen Frequenzen für die jeweilige Auflösung fest. Die Monitoreigenschaften, insbesondere die zulässigen Frequenzen, werden im Abschnitt `Monitor` gespeichert. Standard-VESA-Modi können auch mit dem Dienstprogramm `cvt` generiert werden. Weitere Informationen über cvt erhalten Sie auf der man-Seite `man cvt`.

WARNUNG

Die Modelines sollten Sie nur ändern, wenn Sie sich sehr gut mit den Bildschirmfunktionen und der Grafikkarte auskennen, da der Bildschirm durch eine falsche Änderung dieser Zeilen ernsthaft Schaden nehmen kann.

Falls Sie Ihre eigenen Monitorbeschreibungen entwickeln möchten, sollten Sie sich eingehend mit der Dokumentation unter `/usr/share/X11/doc` vertraut machen. Installieren Sie das Paket `xorg-x11-doc`, um PDFs und HTML-Seiten zu finden.

Heutzutage ist es nur sehr selten erforderlich, Modelines manuell festzulegen. Wenn Sie mit einem modernen Multisync-Monitor arbeiten, können die zulässigen Frequenzen und die optimalen Auflösungen in aller Regel vom X-Server direkt per DDC vom

Monitor abgerufen werden, wie im SaX2-Konfigurationsabschnitt beschrieben. Ist dies aus irgendeinem Grund nicht möglich, können Sie auf einen der VESA-Modi des X-Servers zurückgreifen. Dies funktioniert in Verbindung mit den meisten Kombinationen aus Grafikkarte und Monitor.

12.2 Installation und Konfiguration von Schriften

Die Installation zusätzlicher Schriften unter SUSE® Linux Enterprise Server ist sehr einfach. Kopieren Sie einfach die Schriften in ein beliebiges Verzeichnis im X11-Pfad für Schriften (siehe Abschnitt 12.2.1, „X11 Core-Schriften“ (S. 168)). Damit die Schriften verwendet werden können, sollte das Installationsverzeichnis ein Unterverzeichnis der Verzeichnisse sein, die in `/etc/fonts/fonts.conf` konfiguriert sind (siehe Abschnitt 12.2.2, „Xft“ (S. 169)), oder es sollte über `/etc/fonts/suse-font-dirs.conf` in diese Datei eingefügt worden sein.

Nachfolgend ein Ausschnitt aus der Datei `/etc/fonts/fonts.conf`. Diese Datei ist die Standard-Konfigurationsdatei, die für die meisten Konfigurationen geeignet ist. Sie definiert auch das eingeschlossene Verzeichnis `/etc/fonts/conf.d`. Alle Dateien und symbolischen Links in diesem Verzeichnis, die mit einer zweistelligen Zahl beginnen, werden von fontconfig geladen. Ausführliche Erläuterungen zu dieser Funktion finden Sie in der Datei `/etc/fonts/conf.d/README`.

```
<!-- Font directory list -->
<dir>/usr/share/fonts</dir>
<dir>/usr/X11R6/lib/X11/fonts</dir>
<dir>/opt/kde3/share/fonts</dir>
<dir>/usr/local/share/fonts</dir>
<dir>~/.fonts</dir>
<include ignore_missing="yes">conf.d</include>
```

`/etc/fonts/suse-font-dirs.conf` wird automatisch generiert, um Schriften abzurufen, die mit Anwendungen (meist von anderen Herstellern) wie OpenOffice.org, Java oder Adobe Acrobat Reader geliefert werden. Einige typische Einträge von `/etc/fonts/suse-font-dirs.conf`:

```
<dir>/usr/lib64/ooo-2.0/share/fonts</dir>
<dir>/usr/lib/jvm/java-1_4_2-sun-1.4.2.11/jre/lib/fonts</dir>
<dir>/usr/lib64/jvm/java-1.5.0-sun-1.5.0_07/jre/lib/fonts</dir>
<dir>/usr/X11R6/lib/Acrobat7/Resource/Font</dir>
```

```
<dir>/usr/X11R6/lib/Acrobat7/Resource/Font/PFM</dir>
```

Um zusätzliche Schriften systemweit zu installieren, kopieren Sie Schriftdateien manuell (als `root`) in ein geeignetes Verzeichnis, beispielsweise `/usr/share/fonts/truetype`. Alternativ kann diese Aktion auch mithilfe des KDE-Schrift-Installationsprogramms im KDE-Kontrollzentrum durchgeführt werden. Das Ergebnis ist dasselbe.

Anstatt die eigentlichen Schriften zu kopieren, können Sie auch symbolische Links erstellen. Beispielsweise kann dies sinnvoll sein, wenn Sie lizenzierte Schriften auf einer eingehängten Windows-Partition haben und diese nutzen möchten. Führen Sie anschließend `SuSEconfig --module fonts` aus.

`SuSEconfig --module fonts` startet das für die Schriftenkonfiguration zuständige Skript `/usr/sbin/fonts-config`. Weitere Informationen zu diesem Skript finden Sie auf der man-Seite `man fonts-config`.

Die Vorgehensweise ist für Bitmap-, TrueType- und OpenType-Schriften sowie Type1-Schriften (PostScript) dieselbe. Alle diese Schriften können in einem beliebigen Verzeichnis installiert werden.

X.Org enthält zwei komplett unterschiedliche Schriftsysteme: das alte *X11-Core-Schriftsystem* und das neu entwickelte System *Xft und fontconfig*. In den folgenden Abschnitten wird kurz auf diese beiden Systeme eingegangen.

12.2.1 X11 Core-Schriften

Heute unterstützt das X11 Core-Schriftsystem nicht nur Bitmap-Schriften, sondern auch skalierbare Schriften wie Type1-, TrueType- und OpenType-Schriften. Skalierbare Schriften werden nur ohne Antialiasing und Subpixel-Rendering unterstützt und das Laden von großen skalierbaren Schriften mit Zeichen für zahlreiche Sprachen kann sehr lange dauern. Unicode-Schriften werden ebenfalls unterstützt, aber ihre Verwendung kann mit erheblichem Zeitaufwand verbunden sein und erfordert mehr Speicher.

Das X11 Core-Schriftsystem weist mehrere grundsätzliche Schwächen auf. Es ist überholt und kann nicht mehr sinnvoll erweitert werden. Zwar muss es noch aus Gründen der Abwärtskompatibilität beibehalten werden, doch das modernere System "Xft/fontconfig" sollte immer verwendet werden, wenn es möglich ist.

Der X-Server muss die verfügbaren Schriften und deren Speicherorte im System kennen. Dies wird durch Verwendung der Variablen `FontPath` erreicht, in der die Pfade zu allen gültigen Schriftverzeichnissen des Systems vermerkt sind. In jedem dieser Verzeichnisse sind die dort verfügbaren Schriften in einer Datei mit dem Namen `fonts.dir` aufgeführt. Der `FontPath` wird vom X Server beim Systemstart erzeugt. Der Server sucht an jedem Speicherort, auf den die `FontPath`-Einträge der Konfigurationsdatei `/etc/X11/xorg.conf` verweisen, nach einer gültigen `fonts.dir`-Datei. Diese Einträge befinden sich im Abschnitt `Files`. Der `FontPath` lässt sich mit dem Befehl `xset q` anzeigen. Dieser Pfad kann auch zur Laufzeit mit dem Befehl `xset` geändert werden. Zusätzliche Pfade werden mit `xset+fp <Pfad>` hinzugefügt. Unerwünschte Pfade können mit `xset-fp <Pfad>` gelöscht werden.

Wenn der X-Server bereits aktiv ist, können Sie neu installierte Schriften in eingehängten Verzeichnissen mit dem Befehl `xsetfp rehash` verfügbar machen. Dieser Befehl wird von `SuSEconfig--module fonts` ausgeführt. Da zur Ausführung des Befehls `xset` der Zugriff auf den laufenden X-Server erforderlich ist, ist dies nur möglich, wenn `SuSEconfig--module fonts` von einer Shell aus gestartet wird, die Zugriff auf den laufenden X-Server hat. Am einfachsten erreichen Sie dies, indem Sie `su` und das `root`-Passwort eingeben und dadurch `root`-Berechtigungen erlangen. `su` überträgt die Zugriffsberechtigungen des Benutzers, der den X Server gestartet hat, auf die `root`-Shell. Wenn Sie überprüfen möchten, ob die Schriften ordnungsgemäß installiert wurden und über das X11 Core-Schriftsystem verfügbar sind, geben Sie den Befehl `xlsfonts` ein, um alle verfügbaren Schriften aufzulisten.

Standardmäßig arbeitet SUSE Linux Enterprise Server mit UTF-8-Gebietsschemata. Daher sollten nach Möglichkeit Unicode-Schriften verwendet werden (Schriftnamen, die in der von `xlsfonts` ausgegebenen Liste auf `iso10646-1` enden). Alle verfügbaren Unicode-Schriften lassen sich über den Befehl `xlsfonts | grep iso10646-1` auflisten. Praktisch alle Unicode-Schriften, die unter SUSE Linux Enterprise Server zur Verfügung stehen, umfassen zumindest die für europäische Sprachen erforderlichen Schriftzeichen (früher als `iso-8859-*` kodiert).

12.2.2 Xft

Die Programmierer von Xft haben von Anfang an sichergestellt, dass auch skalierbare Schriften, die Antialiasing nutzen, problemlos unterstützt werden. Bei Verwendung von Xft werden die Schriften von der Anwendung, die die Schriften nutzt, und nicht

vom X-Server gerendert, wie es beim X11 Core-Schriftsystem der Fall ist. Auf diese Weise hat die jeweilige Anwendung Zugriff auf die eigentlichen Schriftdateien und kann genau steuern, wie die Zeichen gerendert werden. Dies bildet eine optimale Basis für die ordnungsgemäße Textdarstellung für zahlreiche Sprachen. Direkter Zugriff auf die Schriftdateien ist sehr nützlich, wenn Schriften für die Druckausgabe eingebettet werden sollen. So lässt sich sicherstellen, dass der Ausdruck genau der Bildschirmdarstellung entspricht.

Unter SUSE Linux Enterprise Server nutzen die beiden Desktop-Umgebungen KDE und GNOME sowie Mozilla und zahlreiche andere Anwendungen bereits standardmäßig Xft. Xft wird inwischen von mehr Anwendungen genutzt als das alte X11 Core-Schriftsystem.

Xft greift für die Suche nach Schriften und für deren Darstellung auf die fontconfig-Bibliothek zurück. Die Eigenschaften von fontconfig werden durch die globale Konfigurationsdatei `/etc/fonts/fonts.conf` gesteuert. Spezielle Konfigurationen sollten zu `/etc/fonts/local.conf` und der benutzerspezifischen Konfigurationsdatei `~/.fonts.conf` hinzugefügt werden. Jede dieser fontconfig-Konfigurationsdateien muss folgendermaßen beginnen:

```
<?xml version="1.0"?>
<!DOCTYPE fontconfig SYSTEM "fonts.dtd">
<fontconfig>
```

Enden müssen die Dateien wie folgt:

```
</fontconfig>
```

Wenn Sie möchten, dass weitere Verzeichnisse nach Schriften durchsucht werden sollen, fügen Sie Zeilen in der folgenden Weise hinzu:

```
<dir>/usr/local/share/fonts/</dir>
```

Dies ist jedoch in der Regel nicht erforderlich. Standardmäßig ist das benutzerspezifische Verzeichnis `~/.fonts` bereits in die Datei `/etc/fonts/fonts.conf` eingetragen. Entsprechend müssen Sie die zusätzlichen Schriften einfach nur nach `~/.fonts` kopieren, um sie zu installieren.

Außerdem können Sie Regeln angeben, die die Darstellung der Schriften beeinflussen. Geben Sie beispielsweise Folgendes ein:

```
<match target="font">
 <edit name="antialias" mode="assign">
```

```
  <bool>false</bool>
 </edit>
</match>
```

Hierdurch wird das Antialiasing für alle Schriften aufgehoben. Wenn Sie hingegen

```
<match target="font">
 <test name="family">
  <string>Luxi Mono</string>
  <string>Luxi Sans</string>
 </test>
 <edit name="antialias" mode="assign">
 <bool>false</bool>
 </edit>
</match>
```

eingeben, wird das Antialiasing nur für bestimmte Schriften aufgehoben.

Standardmäßig verwenden die meisten Anwendungen die Schriftbezeichnungen `sans-serif` (bzw. `sans`), `serif` oder `monospace`. Hierbei handelt es sich nicht um eigentliche Schriften, sondern nur um Aliasnamen, die je nach Spracheinstellung in eine passende Schrift umgesetzt werden.

Benutzer können problemlos Regeln zur Datei `~/.fonts.conf` hinzufügen, damit diese Aliasnamen in ihre bevorzugten Schriften umgesetzt werden:

```
<alias>
 <family>sans-serif</family>
 <prefer>
  <family>FreeSans</family>
 </prefer>
</alias>
<alias>
 <family>serif</family>
 <prefer>
  <family>FreeSerif</family>
 </prefer>
</alias>
<alias>
 <family>monospace</family>
 <prefer>
  <family>FreeMono</family>
 </prefer>
</alias>
```

Da fast alle Anwendungen standardmäßig mit diesen Aliasnamen arbeiten, betrifft diese Änderung praktisch das gesamte System. Daher können Sie nahezu überall sehr einfach Ihre Lieblingsschriften verwenden, ohne die Schrifteinstellungen in den einzelnen Anwendungen ändern zu müssen.

Mit dem Befehl `fc-list` finden Sie heraus, welche Schriften installiert sind und verwendet werden können. Der Befehl `fc-list` gibt eine Liste aller Schriften zurück. Wenn Sie wissen möchten, welche der skalierbaren Schriften (`:scalable=true`) alle erforderlichen Zeichen für Hebräisch (`:lang=he`) enthalten und Sie deren Namen (`family`), Schnitt (`style`) und Stärke (`weight`) sowie die Namen der entsprechenden Schriftdateien anzeigen möchten, geben Sie folgenden Befehl ein:

```
fc-list ":lang=he:scalable=true" family style weight
```

Auf diesen Befehl kann beispielsweise Folgendes zurückgegeben werden:

```
Lucida Sans:style=Demibold:weight=200
DejaVu Sans:style=Bold Oblique:weight=200
Lucida Sans Typewriter:style=Bold:weight=200
FreeSerif:style=Bold,polkrepko:weight=200
FreeSerif:style=Italic,ležeče:weight=80
FreeSans:style=Medium,navadno:weight=80
DejaVu Sans:style=Oblique:weight=80
FreeSans:style=Oblique,ležeče:weight=80
```

In der folgenden Tabelle finden Sie wichtige Parameter, die mit dem Befehl `fc-list` abgefragt werden können:

Tabelle 12.2 *Parameter zur Verwendung mit fc-list*

Parameter	Bedeutung und zulässige Werte
`family`	Der Name der Schriftamilie, z. B. `FreeSans`.
`foundry`	Der Hersteller der Schrift, z. B. `urw`.
`style`	Der Schriftschnitt, z. B. `Medium`, `Regular`, `Bold`, `Italic` oder `Heavy`.
`lang`	Die Sprache, die von dieser Schrift unterstützt wird, z. B. `de` für Deutsch, `ja` für Japanisch, `zh-TW` für traditionelles Chinesisch oder `zh-CN` für vereinfachtes Chinesisch.
`weight`	Die Schriftstärke, z. B. `80` für normale Schrift oder `200` für Fettschrift.

Parameter	Bedeutung und zulässige Werte
slant	Die Schriftneigung, in der Regel 0 für gerade Schrift und 100 für Kursivschrift.
geschrieben werden	Der Name der Schriftdatei.
outline	true für Konturschriften oder false für sonstige Schriften.
scalable	true für skalierbare Schriften oder false für sonstige Schriften.
bitmap	true für Bitmap-Schriften oder false für sonstige Schriften.
pixelsize	Schriftgröße in Pixel. In Verbindung mit dem Befehl "fc-list" ist diese Option nur bei Bitmap-Schriften sinnvoll.

12.3 Weiterführende Informationen

Installieren Sie die Pakete xorg-x11-doc und howtoenh , um detailliertere Informationen zu X11 zu erhalten. Weitere Informationen zur X11-Entwicklung finden Sie auf der Startseite des Projekts unter http://www.x.org.

Viele der Treiber, die mit dem Paket xorg-x11-driver-video geliefert werden, sind ausführlich in einer man-Seite beschrieben. Wenn Sie beispielsweise den Radeon-Treiber verwenden, erhalten Sie weitere Informationen auf der man-Seite man 4 radeon.

Informationen über Treiber von anderen Herstellern sollten in /usr/share/doc/packages/<paketname> zur Verfügung stehen. Beispielsweise ist die Dokumentation von x11-video-nvidiaG01 nach der Installation des Pakets in /usr/share/doc/packages/x11-video-nvidiaG01 verfügbar.

Zugriff auf Dateisysteme mit FUSE

13

FUSE ist das Akronym für *File System in Userspace* (Dateisystem im Benutzerraum). Das bedeutet, Sie können ein Dateisystem als nicht privilegierter Benutzer konfigurieren und einhängen. Normalerweise müssen Sie für diese Aufgabe als `root` angemeldet sein. FUSE alleine ist ein Kernel-Modul. In Kombination mit Plug-Ins kann FUSE auf nahezu alle Dateisysteme wie SSH-Fernverbindungen, ISO-Images und mehr erweitert werden.

13.1 Konfigurieren von FUSE

Bevor Sie FUSE installieren können, müssen Sie das Paket `fuse` installieren. Abhängig vom gewünschten Dateisystem benötigen Sie zusätzliche Plug-Ins in verschiedenen Paketen. Verwenden Sie YaST und die Schlüsselwörter `fuse` oder `Dateisystem` für die Suche nach diesen Paketen.

Im Allgemeinen müssen Sie FUSE nicht konfigurieren, Sie können es einfach verwenden. Jedoch empfiehlt es sich, ein Verzeichnis anzulegen, in dem Sie alle Ihre Einhängepunkte speichern. Sie können beispielsweise das Verzeichnis `~/mounts` anlegen und dort Ihre Unterverzeichnisse für die verschiedenen Dateisysteme einfügen.

13.2 Einhängen einer NTFS-Partition

NTFS, das *New Technology File System*, ist das Standard-Dateisystem von mehreren Windows-Versionen, z. B. Windows NT, 2000, XEP und Vista. Es hat Vorrang vor

den FAT-Dateisystemen. Gehen Sie zum Einhängen einer Windows-Partition als gewöhnlicher Benutzer wie folgt vor:

1. Melden Sie sich als `root` an und installieren Sie das Paket `ntfs-3g`.

2. Legen Sie das Verzeichnis `/media/windows` an.

3. Finden Sie heraus, welche Window-Partition Sie brauchen. Verwenden Sie YaST und starten Sie das Partitionierungsmodul, um zu sehen, welche Partition zu Windows gehört, aber nehmen Sie keine Änderungen vor. Alternativ können Sie sich als `root` anmelden und `/sbin/fdisk -l` ausführen. Suchen Sie Partitionen mit dem Partitionstyp `HPFS/NTFS`.

4. Hängen Sie die Partition im Schreib-Lese-Modus ein. Ersetzen Sie den Platzhalter *`DEVICE`* durch Ihre entsprechende Windows-Partition:

   ```
   ntfs-3g /dev/DEVICE /media/windows
   ```

   Wenn Sie Ihre Windows-Partition im schreibgeschützten Modus verwenden möchten, hängen Sie `-o` an:

   ```
   ntfs-3g /dev/DEVICE /media/windows -o ro
   ```

   Das Kommando `ntfs-3g` verwendet die aktuelle Benutzer- (uid) und Gruppen-ID (gid), um das angegebene Gerät einzuhängen. Wenn Sie die Schreibberechtigungen auf einen anderen Benutzer einstellen möchten, verwenden Sie das Kommando `id USER`, um die Ausgabe der uid- und gid-Werte zu erhalten. Legen Sie ihn fest mit:

   ```
   id tux
   uid=1000(tux) gid=100(users) Gruppen=100(users),16(dialout),33(video)
   ntfs-3g /dev/DEVICE /media/windows -o uid=1000,gid=100
   ```

   Zusätzliche Optionen finden Sie auf der man-Seite.

Verwenden Sie zum Aushängen der Ressource:

```
fusermount -u /media/windows
```

13.3 Einhängen des entfernten Dateisystems mit SSHFS

SSH, das Secure Shell-Netzwerkprotokoll, kann verwendet werden, um Daten zwischen zwei Computern über einen sicheren Kanal auszutauschen. So bauen Sie eine SSH-Verbindung durch FUSE auf:

1. Installieren Sie das Paket `sshfs`.
2. Erstellen Sie ein Verzeichnis, in dem Sie auf den entfernten Computer zugreifen möchten. Eine gute Idee ist die Verwendung von `~/mounts/`*`HOST`*. Ersetzen Sie *`HOST`* durch den Namen Ihres entfernten Computers.
3. Hängen Sie das entfernte Dateisystem ein:

   ```
   sshfs USER:HOST ~/mounts/HOST
   ```

   Ersetzen Sie *`USER`* und *`HOST`* durch Ihre entsprechenden Werte.
4. Geben Sie Ihr Passwort für den entfernten Computer ein.

13.4 Einhängen eines ISO-Dateisystems

Um ein ISO-Image zu untersuchen, können Sie es mit dem Paket `fuseiso` einhängen:

1. Installieren Sie das Paket `fuseiso`.
2. Erstellen Sie das Verzeichnis `~/mounts/iso`.
3. Hängen Sie das ISO-Image ein:

   ```
   fuseiso ISO_IMAGE ~/mounts/iso
   ```

Sie können nur Inhalte aus dem ISO-Image lesen, aber Sie können keine Inhalte zurückschreiben.

13.5 Erhältliche FUSE-Plug-Ins

FUSE hängt von Plug-Ins ab. Die folgende Tabelle führt gängige Plug-Ins auf.

Tabelle 13.1 *Erhältliche FUSE-Plug-Ins*

`fuseiso`	Hängt CD-ROM-Images mit enthaltenen ISO9660-Dateisystemen ein.
`ntfs-3g`	Hängt NTFS-Volumes (mit Lese- und Schreibunterstützung) ein.
`sshfs`	Dateisystem-Client auf der Basis des SSH-Dateiübertragungsprotokolls
`wdfs`	Hängt WebDAV-Dateisysteme ein.

13.6 Weiterführende Informationen

Für weitere Informationen siehe die Homepage `http://fuse.sourceforge.net` von FUSE.

Teil III. Mobile Computer

Mobile Computernutzung mit Linux

14

Die mobile Computernutzung wird meist mit Notebooks, PDAs, Mobiltelefonen und dem Datenaustausch zwischen diesen Geräten in Verbindung gebracht. An Notebooks oder Desktop-Systeme können aber auch mobile Hardware-Komponenten, wie externe Festplatten, Flash-Laufwerke und Digitalkameras, angeschlossen sein. Ebenso zählen zahlreiche Software-Komponenten zu den Bestandteilen mobiler Computerszenarien und einige Anwendungen sind sogar speziell für die mobile Verwendung vorgesehen.

14.1 Notebooks

Die Hardware von Notebooks unterscheidet sich von der eines normalen Desktopsystems. Dies liegt daran, dass hier Kriterien wie Austauschbarkeit, Platzbedarf und Stromverbrauch wichtige Eigenschaften sind. Die Hersteller von mobiler Hardware haben Standardschnittstellen wie PCMCIA (Personal Computer Memory Card International Association), Mini PCI und Mini PCIe entwickelt, die zur Erweiterung der Hardware von Laptops verwendet werden können. Dieser Standard bezieht sich auf Speicherkarten, Netzwerkschnittstellenkarten, ISDN- und Modemkarten sowie externe Festplatten.

TIPP: SUSE Linux Enterprise Server und Tablet PCs

Tablet PCs werden von SUSE Linux Enterprise Server ebenfalls unterstützt. Tablet PCs sind mit einem Touchpad/Grafiktablett ausgestattet. Sie können also anstatt mit Maus und Tastatur die Daten direkt am Bildschirm mit einem Grafiktablettstift oder sogar mit den Fingerspitzen bearbeiten. Installation und Konfiguration erfolgen im Großen und Ganzen wie bei jedem anderen System.

Eine detaillierte Einführung in die Installation und Konfiguration von Tablet PCs finden Sie unter Kapitel 16, *Verwenden von Tablet PCs* (S. 205).

14.1.1 Energieeinsparung

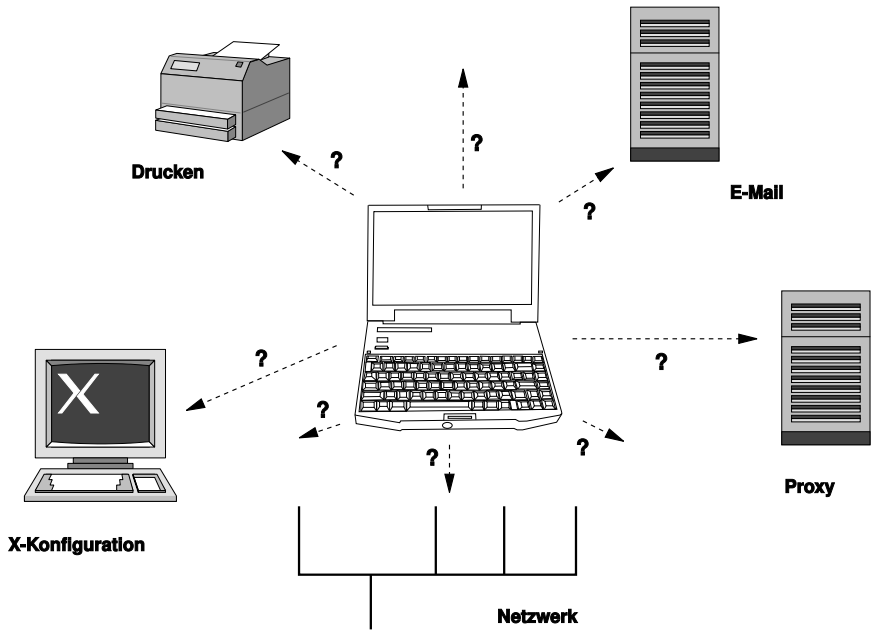
Durch die Integration von energieoptimierten Systemkomponenten bei der Herstellung von Notebooks erhöht sich die Eignung der Geräte für die Verwendung ohne Zugang zum Stromnetz. Ihr Beitrag zur Energieeinsparung ist mindestens so wichtig wie der des Betriebssystems. SUSE® Linux Enterprise Server unterstützt verschiedene Methoden, die den Energieverbrauch eines Notebooks beeinflussen und sich auf die Betriebsdauer bei Akkubetrieb auswirken. In der folgenden Liste werden die Möglichkeiten zur Energieeinsparung in absteigender Reihenfolge ihrer Wirksamkeit angegeben:

- Drosselung der CPU-Geschwindigkeit.
- Ausschalten der Anzeigebeleuchtung während Pausen.
- Manuelle Anpassung der Anzeigebeleuchtung.
- Ausstecken nicht verwendeter, Hotplug-fähiger Zubehörteile (USB-CD-ROM, externe Maus, nicht verwendete PCMCIA-Karten, WLAN usw.).
- Ausschalten der Festplatte im Ruhezustand.

14.1.2 Integration in unterschiedlichen Betriebsumgebungen

Ihr System muss sich an unterschiedliche Betriebsumgebungen anpassen können, wenn es für mobile Computernutzung verwendet werden soll. Viele Dienste hängen von der Umgebung ab und die zugrunde liegenden Clients müssen neu konfiguriert werden. SUSE Linux Enterprise Server übernimmt diese Konfiguration für Sie.

Abbildung 14.1 *Integrieren eines mobilen Computers in eine bestehende Umgebung*



Bei einem Notebook beispielsweise, das zwischen einem kleinen Heimnetzwerk zu Hause und einem Firmennetzwerk hin und her pendelt, sind folgende Dienste betroffen:

Netzwerk
: Dazu gehören IP-Adresszuweisung, Namensauflösung, Internet-Konnektivität und Konnektivität mit anderen Netzwerken.

Druckvorgang
: Die aktuelle Datenbank der verfügbaren Drucker und ein verfügbarer Druckserver (abhängig vom Netzwerk) müssen vorhanden sein.

E-Mail und Proxys
: Wie beim Drucken muss die Liste der entsprechenden Server immer aktuell sein.

X (Grafische Umgebung)
: Wenn das Notebook zeitweise an einen Beamer oder einen externen Monitor angeschlossen ist, müssen die verschiedenen Anzeigekonfigurationen verfügbar sein.

SUSE Linux Enterprise Server bietet verschiedene Möglichkeiten zur Integration eines Notebooks in bestehende Betriebsumgebungen:

NetworkManager
: NetworkManager wurde speziell für die mobile Verbindung von Notebooks mit Netzwerken entwickelt. Dieses Verwaltungsprogramm ermöglicht einen einfachen und automatischen Wechsel zwischen verschiedenen Netzwerkumgebungen oder Netzwerktypen wie WLAN und Ethernet. NetworkManager unterstützt die WEP- und WPA-PSK-Verschlüsselung in drahtlosen LANs. Außerdem werden Einwahlverbindungen (mit smpppd) unterstützt. Beide Desktop-Umgebungen von SUSE Linux (GNOME und KDE) bieten ein Front-End zu NetworkManager. Weitere Informationen zu den Desktop-Applets finden Sie unter Abschnitt 23.4, „Verwenden des KDE-Widgets NetworkManager“ (S. 362) und Abschnitt 23.5, „Verwendung des GNOME NetworkManager-Miniprogramms“ (S. 363).

Tabelle 14.1 *Anwendungsbeispiele für NetworkManager*

Mein Rechner…	NetworkManager verwenden
Der Computer ist ein Notebook.	Ja
Der Computer wird mit verschiedenen Netzwerken verbunden.	Ja
Der Computer stellt Netzwerkdienste bereit (z. B. DNS oder DHCP).	Nein
Der Computer hat eine statische IP-Adresse.	Nein

Verwenden Sie die Werkzeuge von YaST zur Konfiguration der Netzwerkverbindungen, wenn die Netzwerkkonfiguration nicht automatisch von NetworkManager übernommen werden soll.

SCPM

SCPM (System Configuration Profile Management, Verwaltung der Systemkonfigurationsprofile) ermöglicht die Speicherung beliebiger Konfigurationszustände eines Systems in einer Art "Snapshot", die als *Profil* bezeichnet wird. Profile können für verschiedene Situationen erstellt werden. Sie sind nützlich, wenn ein System in unterschiedlichen Umgebungen (Heimnetzwerk, Firmennetzwerk) eingesetzt wird. Ein Umschalten zwischen den Profilen ist jederzeit möglich. Wenn Sie SCPM auf Ihrem System nutzen möchten, installieren Sie das Paket scpm, aktivieren Sie SCPM mithilfe des YaST-Moduls für die Profilverwaltung und konfigurieren Sie die Benutzer, die zwischen den Profilen umschalten können sollen, ohne das `root`-Passwort eingeben zu müssen. Geben Sie an, ob Profiländerungen auch nach dem System-Reboot noch zur Verfügung stehen oder ob Sie beim Herunterfahren verworfen werden sollen. Vergewissern Sie sich, dass sämtliche Ressourcengruppen (etwa Dienste für Netzwerk und Drucker) aktiv sind. Erstellen Sie weiterhin aktuelle Profile mithilfe des Kommandozeilenwerkzeugs `scpm`. Erstellen Sie Profile für all die unterschiedlichen Setups, in denen Sie dieses System verwenden möchten. Für den Wechsel zwischen Profilen gibt es zwei Möglichkeiten: Ausführung des Systems über `scpm` oder Betätigung der Taste `F3` beim Booten des Systems. Beim Umschalten zwischen den Profilen passt SCPM Ihre Systemkonfiguration automa-

tisch an die neue Umgebung an, die in dem von Ihnen ausgewählten Profil erläutert wird.

SLP
: Das Service Location Protocol (SLP) vereinfacht die Verbindung eines Notebooks mit einem bestehenden Netzwerk. Ohne SLP benötigt der Administrator eines Notebooks normalerweise detaillierte Kenntnisse über die im Netzwerk verfügbaren Dienste. SLP sendet die Verfügbarkeit eines bestimmten Diensttyps an alle Clients in einem lokalen Netzwerk. Anwendungen, die SLP unterstützen, können die von SLP weitergeleiteten Informationen verarbeiten und automatisch konfiguriert werden. SLP kann sogar für die Installation eines Systems verwendet werden, wodurch sich die Suche nach einer geeigneten Installationsquelle erübrigt. Weitere Informationen zu SLP finden Sie unter Kapitel 19, *SLP-Dienste im Netzwerk* (S. 299).

14.1.3 Software-Optionen

Bei der mobilen Nutzung gibt es verschiedene spezielle Aufgabenbereiche, die von dedizierter Software abgedeckt werden: Systemüberwachung (insbesondere der Ladezustand des Akkus), Datensynchronisierung sowie drahtlose Kommunikation mit angeschlossenen Geräten und dem Internet. In den folgenden Abschnitten werden die wichtigsten Anwendungen behandelt, die SUSE Linux Enterprise Server für jede Aufgabe bietet.

Systemüberwachung

SUSE Linux Enterprise Server bietet zwei KDE-Werkzeuge zur Systemüberwachung:

KPowersave
: KPowersave ist ein Applet, das den Zustand des Akkus in der Systemsteuerung anzeigt. Das Symbol wird entsprechend der Art der Energieversorgung angepasst. Bei Arbeit mit Wechselstrom wird ein kleines Steckersymbol angezeigt. Bei Arbeit mit Akkustrom wird als Symbol eine Batterie angezeigt. Das zugehörige Menü öffnet das YaST-Modul für die Energieverwaltung nach der Anforderung des `root`-Passworts. Auf diese Weise kann das Verhalten des Systems bei unterschiedlichen Energiequellen festgelegt werden.

KSysguard
: KSysguard ist eine unabhängige Anwendung, die alle messbaren Parameter des Systems in einer einzige Überwachungsumgebung sammelt. KSysguard weist

Monitore für ACPI (Akkustatus), CPU-Last, Netzwerk, Partitionierung und Arbeitsspeicherauslastung. Außerdem kann diese Anwendung alle Systemprozesse überwachen und anzeigen. Die Darstellung und Filterung der gesammelten Daten kann benutzerdefiniert angepasst werden. Es ist möglich, verschiedene Systemparameter auf verschiedenen Datenseiten zu überwachen oder die Daten von mehreren Computern parallel über das Netzwerk zu sammeln. KSysguard kann außerdem als Daemon auf Computern ohne KDE-Umgebung ausgeführt werden. Weitere Informationen zu diesem Programm finden Sie in der zugehörigen integrierten Hilfefunktion bzw. auf den SUSE-Hilfeseiten.

Verwenden Sie auf dem GNOME-Desktop die GNOME-Einstellungen für Energieverwaltung und Systemmonitor.

Datensynchronisierung

Beim ständigen Wechsel zwischen der Arbeit auf einem mobilen Computer, der vom Netzwerk getrennt ist, und der Arbeit an einer vernetzten Arbeitsstation in einem Büro müssen die verarbeiteten Daten stets auf allen Instanzen synchronisiert sein. Dazu gehören E-Mail-Ordner, Verzeichnisse und einzelne Dateien, die sowohl für die Arbeit unterwegs als auch im Büro vorliegen müssen. Die Lösung sieht für beide Fälle folgendermaßen aus:

Synchronisieren von E-Mail
: Verwenden eines IMAP-Kontos zum Speichern der E-Mails im Firmennetzwerk. Der Zugriff auf die E-Mails vom Arbeitsplatzrechner aus erfolgt dann über einen beliebigen, nicht verbundenen IMAP-fähigen E-Mail-Client, wie Mozilla Thunderbird Mail, Evolution oder KMail. Der E-Mail-Client muss so konfiguriert sein, dass für `Sent Messages` (Gesendete Nachrichten) immer derselbe Ordner aufgerufen wird. Dadurch wird gewährleistet, dass nach Abschluss der Synchronisierung alle Nachrichten mit den zugehörigen Statusinformationen verfügbar sind. Verwenden Sie zum Senden von Nachrichten einen im Mail-Client implementierten SMTP-Server anstatt des systemweiten MTA-Postfix oder Sendmail, um zuverlässige Rückmeldungen über nicht gesendete Mail zu erhalten.

Synchronisieren von Dateien und Verzeichnissen
: Es gibt mehrere Dienstprogramme, die sich für die Synchronisierung von Daten zwischen Notebook und Arbeitsstation eignen.

Drahtlose Kommunikation

Neben einem Anschluss an ein Heim- oder Firmennetzwerk über ein Kabel kann ein Notebook auch drahtlos mit anderen Computern, Peripheriegeräten, Mobiltelefonen oder PDAs verbunden sein. Linux unterstützt drei Typen von drahtloser Kommunikation:

WLAN
: WLAN weist die größte Reichweite dieser drahtlosen Technologien auf und ist daher als einziges für den Betrieb großer und zuweilen sogar räumlich geteilter Netzwerke geeignet. Einzelne Computer können untereinander eine Verbindung herstellen und so ein unabhängiges drahtloses Netzwerk bilden oder auf das Internet zugreifen. Als *Zugriffspunkte* bezeichnete Geräte können als Basisstationen für WLAN-fähige Geräte und als Zwischengeräte für den Zugriff auf das Internet fungieren. Ein mobiler Benutzer kann zwischen verschiedenen Zugriffspunkten umschalten, je nachdem, welcher Zugriffspunkt die beste Verbindung aufweist. Wie bei der Mobiltelefonie steht WLAN-Benutzern ein großes Netzwerk zur Verfügung, ohne dass sie für den Zugriff an einen bestimmten Standort gebunden sind. Informationen über WLAN finden Sie in Abschnitt 18.1, „Wireless LAN“ (S. 287).

Bluetooth
: Bluetooth weist das breiteste Anwendungsspektrum von allen drahtlosen Technologien auf. Es kann, ebenso wie IrDA, für die Kommunikation zwischen Computern (Notebooks) und PDAs oder Mobiltelefonen verwendet werden. Außerdem kann es zur Verbindung mehrerer Computer innerhalb des Sichtbereichs verwendet werden. Des Weiteren wird Bluetooth zum Anschluss drahtloser Systemkomponenten, beispielsweise Tastatur und Maus, verwendet. Die Reichweite dieser Technologie reicht jedoch nicht aus, um entfernte Systeme über ein Netzwerk zu verbinden. WLAN ist die optimale Technologie für die Kommunikation durch physische Hindernisse, wie Wände.

IrDA
: IrDA ist die drahtlose Technologie mit der kürzesten Reichweite. Beide Kommunikationspartner müssen sich in Sichtweite voneinander befinden. Hindernisse, wie Wände, können nicht überwunden werden. Eine mögliche Anwendung von IrDA ist die Übertragung einer Datei von einem Notebook auf ein Mobiltelefon. Die kurze Entfernung zwischen Notebook und Mobiltelefon wird mit IrDa überbrückt. Der Langstreckentransport der Datei zum Empfänger erfolgt über das Mobilfunknetz. Ein weiterer Anwendungsbereich von IrDA ist die drahtlose Übertragung von Druckaufträgen im Büro.

14.1.4 Datensicherheit

Idealerweise schützen Sie die Daten auf Ihrem Notebook mehrfach gegen unbefugten Zugriff. Mögliche Sicherheitsmaßnahmen können in folgenden Bereichen ergriffen werden:

Schutz gegen Diebstahl
: Schützen Sie Ihr System stets nach Möglichkeit gegen Diebstahl. Im Einzelhandel ist verschiedenes Sicherheitszubehör, wie beispielsweise Ketten, verfügbar.

Komplexe Authentifizierung
: Verwenden Sie die biometrische Authentifizierung zusätzlich zur standardmäßigen Authentifizierung über Anmeldung und Passwort. SUSE Linux Enterprise Server unterstützt die Authentifizierung per Fingerabdruck. Weitere Informationen finden Sie unter Kapitel 3, *Using the Fingerprint Reader* (↑*Security Guide*).

Sichern der Daten auf dem System
: Wichtige Daten sollten nicht nur während der Übertragung, sondern auch auf der Festplatte verschlüsselt sein. Dies gewährleistet die Sicherheit der Daten im Falle eines Diebstahls. Die Erstellung einer verschlüsselten Partition mit SUSE Linux Enterprise Server wird in Kapitel 12, *Encrypting Partitions and Files* (↑*Security Guide*) beschrieben. Es ist außerdem möglich, verschlüsselte Home-Verzeichnisse beim Hinzufügen des Benutzers mit YaST zu erstellen.

WICHTIG: Datensicherheit und Suspend to Disk

Verschlüsselte Partitionen werden bei Suspend to Disk nicht ausgehängt. Daher sind alle Daten auf diesen Partitionen für jeden verfügbar, dem es gelingt, die Hardware zu stehlen und einen Resume-Vorgang für die Festplatte durchführt.

Netzwerksicherheit
: Jegliche Datenübertragung sollte gesichert werden, gleichgültig auf welche Weise sie erfolgt. Allgemeine, Linux und Netzwerke betreffende Sicherheitsrisiken, sind in Kapitel 1, *Security and Confidentiality* (↑*Security Guide*) beschrieben. Sicherheitsmaßnahmen für drahtlose Netzwerke finden Sie in Kapitel 18, *Drahtlose Kommunikation* (S. 287).

14.2 Mobile Hardware

SUSE Linux Enterprise Server unterstützt die automatische Erkennung mobiler Speichergeräte über FireWire (IEEE 1394) oder USB. Der Ausdruck *mobiles Speichergerät* bezieht sich auf jegliche Arten von FireWire- oder USB-Festplatten, USB-Flash-Laufwerken oder Digitalkameras. Alle Geräte werden automatisch erkannt und konfiguriert, sobald sie mit dem System über die entsprechende Schnittstelle verbunden sind. Die Dateimanager von GNOME und KDE bieten ein flexibles Arbeiten mit mobilen Hardware-Geräten. Verwenden Sie zum sicheren Aushängen dieser Medien folgende Dateiverwaltungsfunktion: *Sicher entfernen* (KDE) bzw. in GNOME die Funktion *Aushängen des Volume*.

Externe Festplatten (USB und FireWire)
: Sobald eine externe Festplatte ordnungsgemäß vom System erkannt wurde, wird das zugehörige Symbol in der Dateiverwaltung angezeigt. Durch Klicken auf das Symbol wird der Inhalt des Laufwerks angezeigt. Sie können hier Ordner und Dateien erstellen, bearbeiten und löschen. Um einer Festplatte einen anderen Namen zu geben als den vom System zugeteilten, wählen Sie das entsprechende Menüelement aus dem Menü aus, das beim Rechtsklicken auf das Symbol geöffnet wird. Die Namensänderung wird nur im Dateimanager angezeigt. Der Deskriptor, durch den das Gerät in `/media` eingehängt wurde, bleibt davon unbeeinflusst.

USB-Flash-Laufwerke
: Diese Geräte werden vom System genau wie externe Festplatten behandelt. Ebenso können Sie die Einträge im Dateimanager umbenennen.

14.3 Mobiltelefone und PDAs

Ein Desktopsystem oder Notebook kann über Bluetooth oder IrDA mit einem Mobiltelefon kommunizieren. Einige Modelle unterstützen beide Protokolle, andere nur eines von beiden. Die Anwendungsbereiche für die beiden Protokolle und die entsprechende erweiterte Dokumentation wurde bereits in „Drahtlose Kommunikation“ (S. 188) erwähnt. Die Konfiguration dieser Protokolle auf den Mobiltelefonen selbst wird in den entsprechenden Handbüchern beschrieben.

Unterstützung für die Synchronisierung mit Handheld-Geräten von Palm, Inc., ist bereits in Evolution und Kontact integriert. Die erstmalige Verbindung mit dem Gerät erfolgt in beiden Fällen problemlos mit der Unterstützung durch einen Assistenten. Sobald die

Unterstützung für Palm Pilots konfiguriert wurde, müssen Sie bestimmen, welche Art von Daten synchronisiert werden soll (Adressen, Termine usw.).

Eine ausgereiftere Lösung zur Synchronisierung ist mit dem Programm `opensync` verfügbar (siehe die Pakete libopensync, msynctool sowie die entsprechenden Plug-Ins für die verschiedenen Geräte).

14.4 Weiterführende Informationen

Die zentrale Informationsquelle für alle Fragen in Bezug auf mobile Geräte und Linux ist `http://tuxmobil.org/`. Verschiedene Bereiche dieser Website befassen sich mit den Hardware- und Software-Aspekten von Notebooks, PDAs, Mobiltelefonen und anderer mobiler Hardware.

Einen ähnlichen Ansatz wie den unter `http://tuxmobil.org/`, finden Sie auch unter `http://www.linux-on-laptops.com/`. Hier finden Sie Informationen zu Notebooks und Handhelds.

SUSE unterhält eine deutschsprachige Mailingliste, die sich mit dem Thema Notebooks befasst. Weitere Informationen hierzu finden Sie unter `http://lists.opensuse.org/opensuse-mobile-de/`. In dieser Liste diskutieren Benutzer alle Aspekte der mobilen Computernutzung mit SUSE Linux Enterprise Server. Einige Beiträge sind auf Englisch, doch der größte Teil der archivierten Informationen liegt in deutscher Sprache vor. `http://lists.opensuse.org/opensuse-mobile/` ist für Beiträge in englischer Sprache vorgesehen.

Informationen über `OpenSync` finden Sie auf `http://en.opensuse.org/OpenSync`.

15 Energieverwaltung

► **zseries:** Die in diesem Kapitel beschriebenen Funktionen und Hardwareelemente sind auf IBM System z nicht vorhanden. Das Kapitel ist für diese Plattformen daher irrelevant. ◄

Die Energieverwaltung ist insbesondere bei Notebook-Computern von großer Wichtigkeit, sie ist jedoch auch für andere Systeme sinnvoll. ACPI (Advanced Configuration and Power Interface) steht auf allen modernen Computern (Laptops, Desktops und Servern) zur Verfügung. Für Energieverwaltungstechnologien sind geeignete Hardware- und BIOS-Routinen erforderlich. Die meisten Notebooks und modernen Desktops und Server erfüllen diese Anforderungen. Es ist außerdem möglich, die CPU-Frequenzskalierung zu steuern, um Energie zu sparen oder den Geräuschpegel zu senken.

15.1 Energiesparfunktionen

Energiesparfunktionen sind nicht nur für die mobile Verwendung von Notebooks von Bedeutung, sondern auch für Desktop-Systeme. Die Hauptfunktionen und ihre Verwendung im ACPI sind:

Standby
: Nicht unterstützt.

Stromsparmodus (in Speicher)
: In diesem Modus wird der gesamte Systemstatus in den RAM geschrieben. Anschließend wird das gesamte System mit Ausnahme des RAM in den Ruhezustand versetzt. In diesem Zustand verbraucht der Computer sehr wenig Energie.

Der Vorteil dieses Zustands besteht darin, dass innerhalb weniger Sekunden die Arbeit nahtlos wieder aufgenommen werden kann, ohne dass ein Booten des Systems oder ein Neustart der Anwendungen erforderlich ist. Diese Funktion entspricht ACPI-Zustand S3. Die Unterstützung für diesen Zustand befindet sich noch in der Entwicklungsphase und hängt daher weitgehend von der Hardware ab.

Tiefschlaf (Suspend to Disk)
: In diesem Betriebsmodus wird der gesamte Systemstatus auf die Festplatte geschrieben und das System wird von der Energieversorgung getrennt. Es muss eine Swap-Partition vorhanden sein, die mindestens die Größe des RAM hat, damit alle aktiven Daten geschrieben werden können. Die Reaktivierung von diesem Zustand dauert ungefähr 30 bis 90 Sekunden. Der Zustand vor dem Suspend-Vorgang wird wiederhergestellt. Einige Hersteller bieten Hybridvarianten dieses Modus an, beispielsweise RediSafe bei IBM Thinkpads. Der entsprechende ACPI-Zustand ist S4. In Linux wird "suspend to disk" über Kernel-Routinen durchgeführt, die von ACPI unabhängig sind.

Akku-Überwachung
: ACPI überprüft den Akkuladestatus und stellt entsprechende Informationen bereit. Außerdem koordiniert es die Aktionen, die beim Erreichen eines kritischen Ladestatus durchzuführen sind.

Automatisches Ausschalten
: Nach dem Herunterfahren wird der Computer ausgeschaltet. Dies ist besonders wichtig, wenn der Computer automatisch heruntergefahren wird, kurz bevor der Akku leer ist.

Steuerung der Prozessorgeschwindigkeit
: In Verbindung mit der CPU gibt es drei Möglichkeiten, Energie zu sparen: Frequenz- und Spannungsskalierung (auch PowerNow! oder Speedstep), Drosselung und Versetzen des Prozessors in den Ruhezustand (C-Status). Je nach Betriebsmodus des Computers können diese Methoden auch kombiniert werden.

15.2 ACPI

ACPI (Advanced Configuration and Power Interface, erweiterte Konfigurations- und Energieschnittstelle) wurde entwickelt, um dem Betriebssystem die Einrichtung und Steuerung der einzelnen Hardware-Komponenten zu ermöglichen. ACPI ersetzt PnP und APM. Diese Schnittstelle bietet Informationen zu Akku, Netzteil, Temperatur,

Ventilator und Systemereignissen wie dem Schließen des Deckels oder einem niedrigen Akkuladestand.

Das BIOS bietet Tabellen mit Informationen zu den einzelnen Komponenten und Hardware-Zugriffsmethoden. Das Betriebssystem verwendet diese Informationen für Aufgaben wie das Zuweisen von Interrupts oder das Aktivieren bzw. Deaktivieren von Komponenten. Da das Betriebssystem die in BIOS gespeicherten Befehle ausführt, hängt die Funktionalität von der BIOS-Implementierung ab. Die Tabellen, die ACPI erkennen und laden kann, werden in `/var/log/boot.msg` gemeldet. Weitere Informationen zur Fehlersuche bei ACPI-Problemen finden Sie in Abschnitt 15.2.3, „Fehlersuche“ (S. 197).

15.2.1 Steuern der CPU-Leistung

Mit der CPU sind Energieeinsparungen auf drei verschiedene Weisen möglich. Je nach Betriebsmodus des Computers können diese Methoden auch kombiniert werden. Energiesparen bedeutet auch, dass sich das System weniger erhitzt und die Ventilatoren seltener in Betrieb sind.

Frequenz- und Spannungsskalierung
: ADM und Intel bezeichnen diese Technologie als PowerNow! und Speedstep. Doch auch in die Prozessoren anderer Hersteller ist diese Technologie integriert. Taktfrequenz und Kernspannung der CPU werden gleichzeitig verringert, was zu mehr als linearen Energieeinsparungen führt. Eine Halbierung der Frequenz (halbe Leistung) führt also dazu, dass wesentlich weniger als die Hälfte der Energie verbraucht wird. Diese Technologie ist unabhängig von ACPI. Es gibt zwei Möglichkeiten, die CPU-Frequenz zu skalieren: über den Kernel selbst oder über eine Userspace-Anwendung. Aus diesem Grund gibt es verschiedene Kernel-Govenors, die in `/sys/devices/system/cpu/cpu*/cpufreq/` festgelegt werden können.

  userspace governor
  : Wenn der Userspace Govrenor eingerichtet wird, steuert der Kernel die CPU-Frequenz durch die Skalierung auf eine Userspace-Anwendung (normalerweise ein Daemon). In SUSE Linux Enterprise Server-Distributionen besteht dieser Daemon im `Powersaved`-Paket. Wenn diese Implementierung verwendet wird, wird die CPU-Frequenz gemäß der aktuellen Systemlast angepasst. Standardmäßig wird eine der Kernel-Implementierungen verwendet. Bei mancher Hardware oder in Bezug auf bestimte Prozessoren oder Treiber ist

die userspace-Implementierung jedoch nach wie vor die einzige funktionierende Lösung.

ondemand governor
: Es handelt sich hierbei um die Kernel-Implementierung einer dynamischen CPU-Frequenz-Richtlinie und sollte auf den meisten Systemen funktionieren. Sobald eine hohe Systemlast vorliegt, wird die CPU-Frequenz sofort erhöht. Sie wird bei einer niedrigeren Systemlast herabgesetzt.

conservative governor
: Dieser Regler ähnelt der On Demand-Implementierung, außer dass eine konservativere Richtlinie verwendet wird. Die Auslastung des Systems muss über einen bestimmten Zeitraum hoch sein, damit die CPU-Frequenz erhöht wird.

powersave governor
: Die CPU-Frequenz wird statisch auf den niedrigsten möglichen Wert gesetzt.

performance governor
: Die CPU-Frequenz wird statisch auf den höchstmöglichen Wert gesetzt.

Drosseln der Taktfrequenz
: Bei dieser Technologie wird ein bestimmter Prozentsatz der Taktsignalimpulse für die CPU ausgelassen. Bei einer Drosselung von 25 % wird jeder vierte Impuls ausgelassen. Bei 87.5 % erreicht nur jeder achte Impuls den Prozessor. Die Energieeinsparungen sind allerdings ein wenig geringer als linear. Normalerweise wird die Drosselung nur verwendet, wenn keine Frequenzskalierung verfügbar ist oder wenn maximale Energieeinsparungen erzielt werden sollen. Auch diese Technologie muss von einem speziellen Prozess gesteuert werden. Die Systemschnittstelle lautet `/proc/acpi/processor/*/throttling`.

Versetzen des Prozessors in den Ruhezustand
: Das Betriebssystem versetzt den Prozessor immer dann in den Ruhezustand, wenn keine Arbeiten anstehen. In diesem Fall sendet das Betriebssystem den Befehl `Halt` an die CPU. Es gibt drei Statusmöglichkeiten: C1, C2 und C3. Im Zustand mit der höchsten Energieeinsparung, C3, wird sogar die Synchronisierung des Prozessor-Cache mit dem Hauptspeicher angehalten. Daher ist dieser Zustand nur möglich, wenn der Inhalt des Hauptspeichers von keinem anderen Gerät über Busmaster-Aktivitäten bearbeitet wird. Einige Treiber verhindern die Verwendung von C3. Der aktuelle Zustand wird unter `/proc/acpi/processor/*/throttling` angezeigt.

Frequenzskalierung und Drosselung sind nur relevant, wenn der Prozessor belegt ist, da der sparsamste C-Zustand ohnehin gilt, wenn sich der Prozessor im Wartezustand befindet. Wenn die CPU belegt ist, ist die Frequenzskalierung die empfohlene Energiesparmethode. Häufig arbeitet der Prozessor nur im Teillast-Betrieb. In diesem Fall kann er mit einer niedrigeren Frequenz betrieben werden. Normalerweise ist eine dynamische Frequenzskalierung, die von dem On Demand-Governor des Kernels oder einem Daemon (z. B. powersaved) gesteuert wird, der beste Ansatz. Eine statische Einstellung auf eine niedrige Frequenz ist sinnvoll bei Akkubetrieb oder wenn der Computer kühl oder geräuscharm arbeiten soll.

Drosselung sollte nur als letzter Ausweg verwendet werden, um die Betriebsdauer des Akkus trotz hoher Systemlast zu verlängern. Einige Systeme arbeiten bei zu hoher Drosselung jedoch nicht reibungslos. Außerdem hat die CPU-Drosselung keinen Sinn, wenn die CPU kaum ausgelastet ist.

15.2.2 ACPI-Werkzeuge

Zu der Palette der mehr oder weniger umfassenden ACPI-Dienstprogramme gehören Werkzeuge, die lediglich Informationen anzeigen, wie beispielsweise Akku-Ladezustand und Temperatur (acpi, klaptopdaemon, usw.), Werkzeuge, die den Zugriff auf die Strukturen unter `/proc/acpi` ermöglichen oder Überwachungsänderungen erleichtern (akpi, acpiw, gtkacpiw), sowie Werkzeuge zum Bearbeiten der ACPI-Tabellen im BIOS (Paket `pmtools`).

15.2.3 Fehlersuche

Es gibt zwei verschiedene Arten von Problemen. Einerseits kann der ACPI-Code des Kernel Fehler enthalten, die nicht rechtzeitig erkannt wurden. In diesem Fall wird eine Lösung zum Herunterladen bereitgestellt. Häufiger jedoch werden die Probleme vom BIOS verursacht. Manchmal werden Abweichungen von der ACPI-Spezifikation absichtlich in das BIOS integriert, um Fehler in der ACPI-Implementierung in anderen weit verbreiteten Betriebssystemen zu umgehen. Hardware-Komponenten, die ernsthafte Fehler in der ACPI-Implementierung aufweisen, sind in einer Blacklist festgehalten, die verhindert, dass der Linux-Kernel ACPI für die betreffenden Komponenten verwendet.

Der erste Schritt, der bei Problemen unternommen werden sollte, ist die Aktualisierung des BIOS. Wenn der Computer sich überhaupt nicht booten lässt, kann eventuell einer der folgenden Bootparameter Abhilfe schaffen:

pci=noacpi
: ACPI nicht zum Konfigurieren der PCI-Geräte verwenden.

acpi=ht
: Nur eine einfache Ressourcenkonfiguration durchführen. ACPI nicht für andere Zwecke verwenden.

acpi=off
: ACPI deaktivieren.

WARNUNG: Probleme beim Booten ohne ACPI

Einige neuere Computer (insbesondere SMP- und AMD64-Systeme) benötigen ACPI zur korrekten Konfiguration der Hardware. Bei diesen Computern kann die Deaktivierung von ACPI zu Problemen führen.

Manchmal ist der Computer durch Hardware gestört, die über USB oder FireWire angeschlossen ist. Wenn ein Computer nicht hochfährt, stecken Sie nicht benötigte Hardware aus und versuchen Sie es erneut.

Überwachen Sie nach dem Booten die Bootmeldungen des Systems mit dem Befehl `dmesg | grep -2i acpi` (oder überwachen Sie alle Meldungen, da das Problem möglicherweise nicht durch ACPI verursacht wurde). Wenn bei der Analyse einer ACPI-Tabelle ein Fehler auftritt, kann die wichtigste Tabelle, DSDT, durch eine verbesserte Version ersetzt werden. In diesem Fall wird die fehlerhafte DSDT des BIOS ignoriert. Das Verfahren wird in Abschnitt 15.4, „Fehlersuche“ (S. 201) erläutert.

In der Kernel-Konfiguration gibt es einen Schalter zur Aktivierung der ACPI-Fehlersuchmeldungen. Wenn ein Kernel mit ACPI-Fehlersuche kompiliert und installiert wurde, können Experten, die nach einem Fehler suchen, mit detaillierten Informationen unterstützt werden.

Wenn Sie Probleme mit dem BIOS oder der Hardware feststellen, sollten Sie stets Kontakt mit den betreffenden Herstellern aufweisen. Insbesondere Hersteller, die nicht immer Hilfe für Linux anbieten, sollten mit den Problemen konfrontiert werden. Die

Hersteller nehmen das Problem nur dann ernst, wenn sie feststellen, dass eine nennenswerte Zahl ihrer Kunden Linux verwendet.

Weiterführende Informationen

- `http://www.cpqlinux.com/acpi-howto.html` (detailliertes ACPI HOWTO, enthält DSDT-Patches)
- `http://www.intel.com/technology/iapc/acpi/index.htm` (ACPI, Advanced Configuration & Power Interface)
- `http://www.lesswatts.org/projects/acpi/` (das ACPI4Linux-Projekt von Sourceforge)
- `http://www.poupinou.org/acpi/` (DSDT-Patches von Bruno Ducrot)

15.3 Ruhezustand für Festplatte

In Linux kann die Festplatte vollständig ausgeschaltet werden, wenn sie nicht benötigt wird, oder sie kann in einem energiesparenderen oder ruhigeren Modus betrieben werden. Bei moderenen Notebooks müssen die Festplatten nicht manuell ausgeschaltet werden, da sie automatisch in einen Sparbetriebsmodus geschaltet werden, wenn sie nicht benötigt werden. Um die Energieeinsparungen zu maximieren, sollten Sie jedoch einige der folgenden Verfahren ausprobieren.

Mit der Anwendung hdparm können verschiedene Festplatteneinstellungen bearbeitet werden. Die Option `-y` schaltet die Festplatte sofort in den Stand-by-Modus. `-Y` versetzt sie in den Ruhezustand. `hdparm -S x` führt dazu, dass die Festplatte nach einen bestimmten Inaktivitätszeitraum abgeschaltet wird. Ersetzen Sie *x* wie folgt: `0` deaktiviert diesen Mechanismus, sodass die Festplatte kontinuierlich ausgeführt wird. Werte von `1` bis `240` werden mit 5 Sekunden multipliziert. Werte von `241` bis `251` entsprechen 1- bis 11-mal 30 Minuten.

Die internen Energiesparoptionen der Festplatte lassen sich über die Option `-B` steuern. Wählen Sie einen Wert `0` (maximale Energieeinsparung) bis `255` (maximaler Durchsatz). Das Ergebnis hängt von der verwendeten Festplatte ab und ist schwer einzuschätzen.

Die Geräuschentwicklung einer Festplatte können Sie mit der Option `-M` reduzieren. Wählen Sie einen Wert von `128` (ruhig) bis `254` (schnell).

Häufig ist es nicht so einfach, die Festplatte in den Ruhezustand zu versetzen. Bei Linux führen zahlreiche Prozesse Schreibvorgänge auf der Festplatte durch, wodurch diese wiederholt aus dem Ruhezustand reaktiviert wird. Daher sollten Sie unbedingt verstehen, wie Linux mit Daten umgeht, die auf die Festplatte geschrieben werden müssen. Zunächst werden alle Daten im RAM-Puffer gespeichert. Dieser Puffer wird vom pdflush-Daemon überwacht. Wenn die Daten ein bestimmtes Alter erreichen oder wenn der Puffer bis zu einem bestimmten Grad gefüllt ist, wird der Pufferinhalt auf die Festplatte übertragen. Die Puffergröße ist dynamisch und hängt von der Größe des Arbeitsspeichers und von der Systemlast ab. Standardmäßig werden für pdflush kurze Intervalle festgelegt, um maximale Datenintegrität zu erreichen. Das Programm überprüft den Puffer alle fünf Sekunden und schreibt die Daten auf die Festplatte. Die folgenden Variablen sind interessant:

`/proc/sys/vm/dirty_writeback_centisecs`
: Enthält die Verzögerung bis zur Reaktivierung eines pdflush-Threads in Hundertstelsekunden.

`/proc/sys/vm/dirty_expire_centisecs`
: Definiert, nach welchem Zeitabschnitt eine schlechte Seite spätestens ausgeschrieben werden sollte. Der Standardwert ist 3000, was 30 Sekunden bedeutet.

`/proc/sys/vm/dirty_background_ratio`
: Maximaler Prozentsatz an schlechten Seiten, bis pdflush damit beginnt, sie zu schreiben. Der Standardwert ist 5 %.

`/proc/sys/vm/dirty_ratio`
: Wenn die schlechten Seiten diesen Prozentsatz des gesamten Arbeitsspeichers überschreiten, werden Prozesse gezwungen, während ihres Zeitabschnitts Puffer mit schlechten Seiten anstelle von weiteren Daten zu schreiben.

WARNUNG: Beeinträchtigung der Datenintegrität

Änderungen an den Einstellungen für den pdflush-Aktualisierungs-Daemon gefährden die Datenintegrität.

Abgesehen von diesen Prozessen schreiben protokollierende Journaling-Dateisysteme, wie ReiserFS und Ext3, ihre Metadaten unabhängig von pdflush, was ebenfalls das

Abschalten der Festplatte verhindert. Um dies zu vermeiden, wurde eine spezielle Kernel-Erweiterung für mobile Geräte entwickelt. Details finden Sie unter `/usr/src/linux/Documentation/laptop-mode.txt`.

Ein weiterer wichtiger Faktor ist die Art und Weise, wie sich die Programme verhalten. Gute Editoren beispielsweise schreiben regelmäßig verborgene Sicherungskopien der aktuell bearbeiteten Datei auf die Festplatte, wodurch die Festplatte wieder aktiviert wird. Derartige Funktionen können auf Kosten der Datenintegrität deaktiviert werden.

In dieser Verbindung verwendet der Mail-Daemon postfix die Variable `POSTFIX_LAPTOP`. Wenn diese Variable auf `yes` (ja) gesetzt wird, greift postfix wesentlich seltener auf die Festplatte zu.

In SUSE Linux Enterprise Server werden diese Techniken durch `laptop-mode-tools` gesteuert.

15.4 Fehlersuche

Alle Fehler- und Alarmmeldungen werden in der Datei `/var/log/messages` protokolliert. Wenn Sie die benötigten Informationen nicht finden können, erhöhen Sie die Ausführlichkeit der Powersave-Meldungen mithilfe von `DEBUG` in der Datei `/etc/sysconfig/powersave/common`. Erhöhen Sie den Wert der Variablen auf `7` oder sogar `15` und starten Sie den Daemon erneut. Mithilfe der detaillierteren Fehlermeldungen in `/var/log/messages` sollten Sie den Fehler leicht finden können. In den folgenden Abschnitten werden die häufigsten Probleme mit Powersave und den verschiedenen Energiesparmodi behandelt.

15.4.1 ACPI mit Hardware-Unterstützung aktiviert, bestimmte Funktionen sind jedoch nicht verfügbar

Bei Problemen mit ACPI können Sie mit dem Befehl `dmesg|grep -i acpi` die Ausgabe von `dmesg` nach ACPI-spezifischen Meldungen durchsuchen. Zur Behebung des Problems kann eine BIOS-Aktualisierung erforderlich sein. Rufen Sie die Homepage Ihres Notebookherstellers auf, suchen Sie nach einer aktualisierten BIOS-Version und

installieren Sie sie. Bitten Sie den Hersteller, die aktuellsten ACPI-Spezifikationen einzuhalten. Wenn der Fehler auch nach der BIOS-Aktualisierung noch besteht, gehen Sie wie folgt vor, um die fehlerhafte DSDT-Tabelle im BIOS mit einer aktualisierten DSDT zu ersetzen:

1. Laden Sie die DSDT für Ihr System von der Seite `http://acpi.sourceforge.net/dsdt/index.php` herunter. Prüfen Sie, ob die Datei dekomprimiert und kompiliert ist. Dies wird durch die Dateinamenserweiterung `.aml` (ACPI Machine Language) angezeigt. Wenn dies der Fall ist, fahren Sie mit Schritt 3 fort.

2. Wenn die Dateierweiterung der heruntergeladenen Tabelle `.asl` (ACPI Source Language) lautet, kompilieren Sie sie mit iasl (Paket `pmtools`). Geben Sie das Kommando `iasl -sa file.asl` ein.

3. Kopieren Sie die Datei `DSDT.aml` an einen beliebigen Speicherort (`/etc/DSDT.aml` wird empfohlen). Bearbeiten Sie `/etc/sysconfig/kernel` und passen Sie den Pfad zur DSDT-Datei entsprechend an. Starten Sie `mkinitrd` (Paket `mkinitrd`). Immer wenn Sie den Kernel installieren und `mkinitrd` verwenden, um `initrd` zu erstellen, wird die bearbeitete DSDT beim Booten des Systems integriert und geladen.

15.4.2 CPU-Frequenzsteuerung funktioniert nicht

Rufen Sie die Kernel-Quelle (`kernel-source`) auf, um festzustellen, ob der verwendete Prozessor unterstützt wird. Möglicherweise ist ein spezielles Kernel-Modul bzw. eine Moduloption erforderlich, um die CPU-Frequenzsteuerung zu aktivieren. Diese Informationen erhalten Sie unter `/usr/src/linux/Documentation/cpu-freq/*`.

15.4.3 Suspend und Stand-by funktionieren nicht

ACPI-Systeme können Probleme mit dem Stromspar- und Standby-Modus haben, wenn die DSDT-Implementierung (BIOS) fehlerhaft ist. Aktualisieren Sie in diesem Fall das BIOS.

Beim Versuch fehlerhafte Module zu entladen, reagiert das System nicht mehr oder das Suspend-Ereignis wird nicht ausgelöst. Dies kann auch dann passieren, wenn Sie keine Module entladen oder Dienste stoppen, die ein erfolgreiches Suspend-Ereignis verhindern. In beiden Fällen müssen Sie versuchen, das fehlerhafte Modul zu ermitteln, das den Energiesparmodus verhindert hat. Die Protokolldatei `/var/log/pm-suspend.log` enthält ausführliche Informationen über die einzelnen Vorgänge und mögliche Fehlerursachen. Ändern Sie die Variable `SUSPEND_MODULES` in `/usr/lib/pm-utils/defaults`, um problematische Module vor einem Suspend- oder Standby-Vorgang zu entladen.

Ausführliche Informationen zur Änderung des Suspend- und Resume-Prozesses finden Sie unter `http://www.opensuse.org/Pm-utils` und `http://www.opensuse.org/S2ram`.

15.5 Weiterführende Informationen

- `http://www.opensuse.org/S2ram` – Anleitung zur Einstellung von "Suspend to RAM"
- `http://www.opensuse.org/Pm-utils` – Anleitung zur Änderung des allgemeinen Suspend-Frameworks

16 Verwenden von Tablet PCs

SUSE® Linux Enterprise Server wird mit Unterstützung für Tablet PCs geliefert. Sie erfahren im Folgenden, wie Sie Ihren Tablet PC installieren und konfigurieren. Außerdem werden Ihnen einige Linux*-Anwendungen vorgestellt, die die Eingabe über digitale Pens akzeptieren.

Die folgenden Tablet PCs werden unterstützt:

- Tablet PCs mit seriellen Wacom-Geräten, z. B. ACER TM C30x-Serie, Fujitsu Lifebook T-Serie (T30xx/T40xx/T50xx), Gateway C-140X/E-295C, HP Compaq TC1100/TC4200/TC4400, 2710p/2730p , IBM/Lenovo X41t/X61t, LG LT20, Motion M1200/M1400, OQO 02, Panasonic Toughbook CF-18, Toshiba Portege/Tecra M-Serie, Satellite R15/R20.
- Tablet PCs mit Wacom-USB-Geräten, z. B. ASUS R1E/R1F, Gateway C-120X/E-155C, HP Pavilion tx2000/tx2100/tx2500-Serie.
- Tablet PCs mit FinePoint-Geräten, z. B. Gateway C210X/M280E/CX2724, HP Compaq TC1000.
- Tablet PCs mit Touchscreen-Geräten, z. B. Asus R2H, Clevo TN120R, Fujitsu Siemens Computers P-Serie, LG C1, Samsung Q1/Q1-Ultra.

Nach der Installation der Tablet PC-Pakete und der Konfiguration Ihres Grafiktabletts können Sie Ihren Pen (auch als Stylus bezeichnet) für folgende Aktionen und Anwendungen verwenden:

- Anmelden bei KDM oder GDM
- Aufheben der Bildschirmsperre auf KDE- und GNOME-Desktops
- Aktionen, die auch durch andere Zeigegeräte (z. B. Maus oder Touch Pad) ausgelöst werden können, wie das Verschieben des Cursors auf dem Bildschirm, das Starten von Anwendungen, das Schließen, Skalieren und Verschieben von Fenstern, den Fokuswechsel in ein anderes Fenster oder das Ziehen und Ablegen von Objekten
- Verwenden der Bewegungserkennung in Anwendungen des X Window System
- Zeichnen mit The GIMP
- Aufzeichnen von Notizen oder Skizzen mit Anwendungen wie Jarnal oder Xournal oder Bearbeiten größerer Textmengen mit Dasher

ANMERKUNG: Tastatur oder Maus für Installation erforderlich

Während der Installation von SUSE Linux Enterprise Server kann der Pen nicht als Eingabegerät verwendet werden. Falls Ihr Tablet PC weder über Tastatur noch Touch Pad verfügt, schließen Sie für die Systeminstallation eine externe Tastatur oder Maus an den Tablet PC an.

16.1 Installieren der Tablet PC-Pakete

Die für Tablet PCs benötigten Pakete sind im Installationsschema `TabletPC` enthalten – wenn dieses Schema während der Installation ausgewählt wurde, sollten die folgenden Pakete bereits auf dem System installiert sein:

- `cellwriter`: eine auf Zeichen basierende Kontrollleiste für handschriftliche Eingabe
- `jarnal`: Eine Java-basierte Anwendung für die Aufzeichnung von Notizen

- `wacom-kmp(-default)`: Der Kernel-Treiber für Tablet PCs mit USB-Wacom-Geräten
- `xournal`: Eine Anwendung für die Aufzeichnung von Notizen und Skizzen
- `xstroke`: Ein Bewegungserkennungsprogramm für das X Window System
- `xvkbd`: Eine virtuelle Tastatur für das X Window System
- `x11-input-fujitsu`: Das X-Eingabemodul für Fujitsu P-Series-Tablets
- `x11-input-evtouch`: Das X-Eingabemodul für einige Tablet PCs mit Touchscreen
- `x11-input-wacom`: Das X-Eingabemodul für Wacom-Tablets
- `x11-input-wacom-tools`: Konfiguration, Diagnose und Bibliotheken für Wacom-Tablets

Falls diese Pakete noch nicht installiert sind, installieren Sie diejenigen Pakete, die Sie benötigen, manuell über die Kommandozeile oder wählen Sie das Schema `TabletPC` in YaST zur Installation aus.

16.2 Konfigurieren des Tablet-Geräts

Sie können Ihren Tablet PC (mit Ausnahme von Tablet PCs mit Touchscreens) während des Installationsvorgangs im Fenster *Hardware-Konfiguration* konfigurieren, indem Sie die Optionen für die *Grafikkarte* ändern. Alternativ können Sie das (interne oder externe) Tablet-Gerät jederzeit nach der Installation konfigurieren.

1. Starten Sie SaX2 an der Kommandozeile oder drücken Sie Alt + F2 und geben Sie `sax2` ein.
2. Klicken Sie bei einem Wacom- oder Finepoint-Gerät auf *Tablet*, um die *Tablet-Eigenschaften* anzuzeigen.

   Wenn Sie einen Tablet PC mit einem Touchscreen verwenden, klicken Sie stattdessen auf *Touchscreen*.

3. Wählen Sie in der Liste auf der rechten Seite *TABLET PCs* als Hersteller und den Namen Ihres Tablets aus und aktivieren Sie *Dieses Tablet aktivieren*.

   Wenn Ihr Computer nicht aufgelistet ist und Sie nicht sicher sind, ob Sie ein Wacom-Gerät besitzen, wählen Sie *Wacom ISDV4 Tablet PC (SERIAL)* oder *Wacom ISDV4 Tablet PC (USB)* aus.

4. Öffnen Sie den Karteireiter *Elektronische Stifte* und aktivieren Sie dort die folgenden Optionen: *Stift hinzufügen* und *Radierer hinzufügen*. Wenn Sie einen Tablet PC mit Touchscreen verwenden, aktivieren Sie auch *Touch hinzufügen*.

5. Klicken Sie zum Speichern der Änderungen auf *OK*.

Starten Sie Ihren X Server nach Abschluss der X Window System-Konfiguration neu, indem Sie sich abmelden. Alternativ können Sie die Benutzeroberfläche auch geöffnet lassen und `init 3 && init 5` in einer virtuellen Konsole ausführen.

Nach der Konfiguration Ihres Tablet-Geräts können Sie nun den Stift (bzw. Ihren Finger, abhängig von Ihrem Tablet PC) als Eingabegerät benutzen.

16.3 Verwenden der virtuellen Tastatur

Zur Anmeldung beim KDE- oder GNOME-Desktop und zum Entsperren des Bildschirms können Sie Ihren Benutzernamen und Ihr Passwort wie gewohnt eingeben oder Sie können dazu die virtuelle Tastatur (xvkbd) verwenden, die sich unterhalb des Anmeldefelds befindet. Zur Konfiguration der Tastatur und zum Aufrufen der integrierten Hilfe klicken Sie links unten auf das Feld *xvkbd*, um das xvkbd-Hauptmenü zu öffnen.

Wenn Ihre Eingabe nicht sichtbar ist (oder nicht an das entsprechende Fenster übertragen wird), lenken Sie den Fokus um, indem Sie auf die *Fokus*-Taste in xvkbd und dann in das Fenster klicken, das die Tastaturereignisse empfangen soll.

Abbildung 16.1 *Virtuelle Tastatur von xvkbd*

xvkbd (v3.0)
F1 F2 F3 F4 F5 F6 F7 F8 F9 F10 F11 F12 Backspace
Esc 1 2 3 4 5 6 7 8 9 0 Tab Q W E R T Y U I O P Del
Control A S D F G H J K L Return
Shift Z X C V B N M Compose Shift
xvkbd Caps Lock Alt Meta Meta Alt Focus
Num Lock / * Focus
7 Home 8 Up 9 PgUp +
4 Left 5 6 Right -
1 End 2 Down 3 PgDn Enter
0 Ins . Del

Wenn Sie xvkbd nach der Anmeldung verwenden möchten, starten Sie es aus dem Hauptmenü oder über das Shell-Kommando `xvkbd`.

16.4 Drehen der Ansicht

Verwenden Sie KRandRTray (KDE) oder gnome-display-properties (GNOME), um Ihre Anzeige manuell interaktiv zu drehen oder die Größe zu verändern. Sowohl KRandRTray als auch gnome-display-properties sind Miniprogramme für die RANDR-Erweiterung von X Server.

Starten Sie KRandRTray oder gnome-display-properties im Hauptmenü oder geben Sie `krandrtray` oder `gnome-display-properties` ein, um das Miniprogramm von einer Shell aus zu starten. Nach Starten des entsprechenden Miniprogramms wird das Symbol für das Miniprogramm gewöhnlich zum Systemabschnitt der Kontrollleiste hinzugefügt. Wenn das gnome-display-properties-Symbol nicht automatisch im Systemabschnitt der Kontrollleiste angezeigt wird, stellen Sie sicher, dass *Show Displays in Panel* (Symbole in Kontrollleisten anzeigen) im Dialogfeld *Monitor Resolution Settings* (Einstellungen für Monitorauflösung) aktiviert ist.

Zum Drehen Ihrer Anzeige mit KRandRTray klicken Sie mit der rechten Maustaste auf das Symbol und wählen Sie *Anzeige konfigurieren*. Wählen Sie die gewünschte Ausrichtung im Konfigurations-Dialogfeld aus.

Zum Drehen Ihrer Anzeige mit gnome-display-properties klicken Sie mit der rechten Maustaste auf das Symbol und wählen Sie die gewünschte Ausrichtung aus. Die Ansicht wird sofort gedreht. Gleichzeitig ändert sich auch die Ausrichtung des Grafiktabletts. Es kann daher die Bewegungen des Pens nach wie vor richtig interpretieren.

Bei Problemen mit der Ausrichtung Ihres Desktops finden Sie weitere Informationen unter Abschnitt 16.7, „Fehlersuche“ (S. 215).

16.5 Verwenden der Bewegungserkennung

SUSE Linux Enterprise Server umfasst CellWriter und xstroke zur Bewegungserkennung. Beide Anwendungen akzeptieren Bewegungen mit dem Stift oder anderen Zeigegeräten als Eingabe für Anwendungen auf dem X Window System.

16.5.1 Verwenden von CellWriter

Mit CellWriter können Sie Zeichen in ein Zellraster schreiben – die Eingabe wird sofort auf Zeichenbasis erkannt. Nachdem Sie die Eingabe beendet haben, können Sie die Eingabe an die aktuell fokussierte Anwendung schicken. Bevor Sie CellWriter zur Bewegungserkennung nutzen können, muss die Anwendung zur Erkennung Ihrer Handschrift trainiert werden: Sie müssen jedes Zeichen anhand einer Zeichentabelle trainieren (nicht trainierte Zeichen werden nicht aktiviert und können daher nicht benutzt werden).

Prozedur 16.1 *Trainieren von CellWriter*

1. CellWriter starten Sie aus dem Hauptmenü oder von der Kommandozeile mit dem Kommando `cellwriter`. Beim ersten Start beginnt CellWriter automatisch im Trainingsmodus. Im Trainingsmodus wird ein Satz von Zeichen aus der aktuell ausgewählten Tastaturbelegung angezeigt.

2. Führen Sie die gewünschte Bewegung für ein Zeichen in der entsprechenden Zelle des Zeichens aus. Mit der ersten Eingabe ändert der Hintergrund seine Farbe in Weiß, während das Zeichen selbst in Hellgrau angezeigt wird. Wiederholen Sie die Bewegung mehrmals, bis das Zeichen in Schwarz angezeigt wird. Nicht trainierte Zeichen werden auf hellgrauem oder braunem Hintergrund (abhängig vom Farbschema auf dem Desktop) angezeigt.

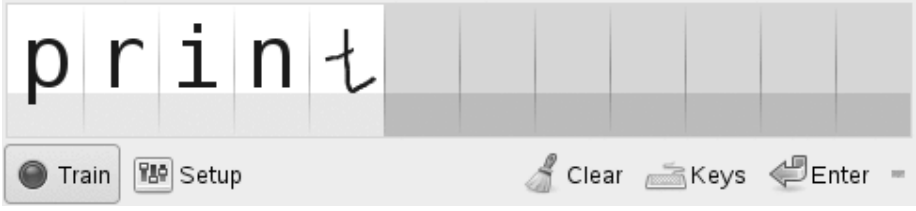
3. Wiederholen Sie diesen Schritt, bis Sie CellWriter für alle benötigten Zeichen trainiert haben.

4. Wenn Sie CellWriter für eine andere Sprache trainieren möchten, klicken Sie auf die Schaltfläche *Setup* und wählen Sie eine Sprache in der Registerkarte *Sprachen* aus. *Schließen* Sie das Konfigurationsdialogfeld. Klicken Sie auf die Schaltfläche *Train* (Trainieren) und wählen Sie die Zeichentabelle aus dem Dropdown-Feld in der unteren rechten Ecke des *CellWriter*-Fensters. Wiederholen Sie nun Ihr Training für die neue Zeichentabelle.

5. Nachdem Sie das Training für die Zeichentabelle abgeschlossen haben, klicken Sie auf die Schaltfläche *Train* (Trainieren), um in den normalen Modus zu wechseln.

Im normalen Modus zeigen die CellWriter-Fenster ein paar leere Zellen, in die die Bewegungen einzugeben sind. Die Zeichen werden erst dann an eine andere Anwendung gesendet, wenn Sie auf die Schaltfläche *Eingabe* klicken, Sie können also Zeichen korrigieren oder löschen, bevor Sie sie als Eingabe verwenden. Zeichen, die mit geringer Zuverlässigkeit erkannt wurden, werden markiert. Verwenden Sie zur Korrektur Ihrer Eingabe das Kontextmenü, das Sie öffnen, indem Sie mit der rechten Maustaste in eine Zelle klicken. Um ein Zeichen zu löschen, verwenden Sie entweder den Radierer Ihres Stifts oder klicken Sie mit der mittleren Maustaste, um die Zelle zu löschen. Wenn Ihre Eingabe in CellWriter beendet ist, definieren Sie die Anwendung, die die Eingabe empfangen soll, indem Sie in das Fenster der Anwendung klicken. Senden Sie dann die Eingabe an die Anwendung, indem Sie auf *Eingabe* klicken.

Abbildung 16.2 *Bewegungserkennung mit CellWriter*



Wenn Sie auf die Schaltfläche *Tasten* in CellWriter klicken, erhalten Sie eine virtuelle Tastastur, die Sie anstelle der Handschrifterkennung verwenden können.

Um CellWriter auszublenden, schließen Sie das CellWriter-Fenster. Die Anwendung erscheint nun als Symbol in Ihrem Systemabschnitt. Um das Eingabefenster erneut anzuzeigen, klicken Sie auf das Symbol im Systemabschnitt.

16.5.2 Verwenden von Xstroke

xstroke erkennt Bewegungen des Pens oder anderer Zeigegeräte als Eingabe für Anwendungen des X Window System. Das xstroke-Alphabet ist ein mit dem Graffiti*-Alphabet vergleichbares Unistroke-Alphabet. Wenn aktiviert, sendet xstroke die Eingabe an das Fenster, das aktuell den Fokus hält.

1. Starten Sie xstroke aus dem Hauptmenü oder über das Shell-Kommando `xstroke`. Dadurch wird dem Systemabschnitt der Kontrollleiste ein Bleistiftsymbol hinzugefügt.

2. Starten Sie die Anwendung, in die Sie mittels des Pens einen Text eingeben möchten (z. B. ein Terminalfenster, einen Texteditor oder einen OpenOffice.org Writer).

3. Zum Aktivieren der Bewegungserkennung klicken Sie einmal auf das Bleistiftsymbol.

4. Führen Sie auf dem Grafiktablett einige Bewegungen mit dem Pen oder einem anderen Zeigegerät aus. xstroke erfasst die Bewegungen und überträgt sie als Text in das fokussierte Anwendungsfenster.

5. Wenn Sie den Fokus in ein anderes Fenster wechseln möchten, klicken Sie mit dem Pen auf das betreffende Fenster und warten Sie einen Moment (oder verwenden Sie dazu das im Kontrollzentrum des Desktops festgelegte Tastenkürzel).

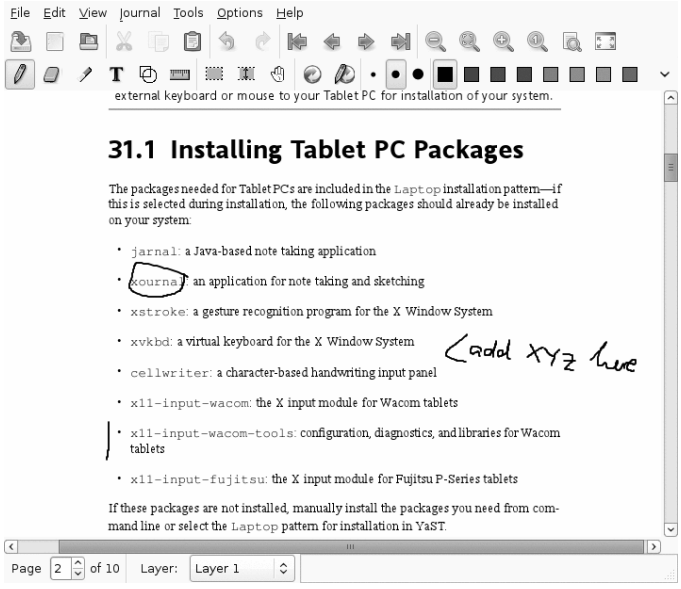
6. Zum Deaktivieren der Bewegungserkennung klicken Sie erneut auf das Bleistiftsymbol.

16.6 Aufzeichnen von Notizen und Skizzen mit dem Pen

Zum Anfertigen von Zeichnungen mit dem Pen können Sie einen professionellen Grafikeditor wie The GIMP oder eine Notizenanwendung wie Xournal oder Jarnal verwenden. Sowohl mit Xournal als auch mit Jarnal können Sie mittels Pen Notizen aufzeichnen, Zeichnungen erstellen oder PDF-Dateien kommentieren. Die Java-basierte Anwendung Jarnal ist für verschiedene Plattformen verfügbar und bietet grundlegende Funktionen der Zusammenarbeit. Weitere Informationen hierzu finden Sie in `http://www.dklevine.com/general/software/tc1000/jarnal-net.htm`. Jarnal speichert den Inhalt in einem Archiv mit der Erweiterung .jaj. Dieses Archiv enthält auch eine Datei im SVG-Format.

Starten Sie Jarnal oder Xournal aus dem Hauptmenü oder über das Shell-Kommando `jarnal` bzw. `xournal`. Wenn Sie zum Beispiel in Xournal eine PDF-Datei kommentieren möchten, wählen Sie *File (Datei) > Annotate PDF (PDF kommentieren)* und öffnen Sie dann die PDF-Datei in Ihrem Dateisystem. Tragen Sie Ihre Kommentare mit dem Pen oder einem anderen Zeigegerät in die PDF-Datei ein und speichern Sie die Änderungen mit *File (Datei) > Print to PDF* (PDF-Ausgabe).

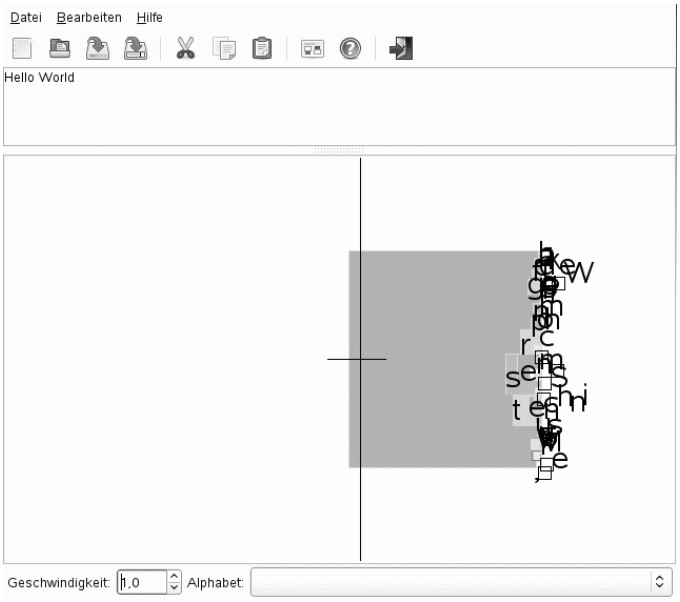
Abbildung 16.3 *Kommentieren einer PDF-Datei mit Xournal*


File Edit View Journal Tools Options Help
external keyboard or mouse to your Tablet PC for installation of your system.
31.1 Installing Tablet PC Packages
The packages needed for Tablet PCs are included in the Laptop installation pattern—if this is selected during installation, the following packages should already be installed on your system:
jarnal: a Java-based note taking application
xournal: an application for note taking and sketching
xstroke: a gesture recognition program for the X Window System
xvkbd: a virtual keyboard for the X Window System
cellwriter: a character-based handwriting input panel
x11-input-wacom: the X input module for Wacom tablets
x11-input-wacom-tools: configuration, diagnostics, and libraries for Wacom tablets
x11-input-fujitsu: the X input module for Fujitsu P-Series tablets
If these packages are not installed, manually install the packages you need from command line or select the Laptop pattern for installation in YaST.
Page 2 of 10
Layer: Layer 1

Dasher ist eine weitere nützliche Anwendung. Sie wurde speziell für Situationen entwickelt, in denen die Eingabe über die Tastatur unpraktisch oder unmöglich ist. Mit ein wenig Übung gelingt es recht bald, auch große Textmengen nur mit dem Pen (oder einem anderen Eingabegerät – selbst mit einem Eye Tracker) einzugeben.

Starten Sie Dasher aus dem Hauptmenü oder über das Shell-Kommando `dasher`. Sobald Sie den Pen in eine Richtung verschieben, beginnen die Buchstaben auf der rechten Seite vorbeizuzoomen. Aus den Buchstaben, die an dem Fadenkreuz in der Mitte vorbeilaufen, wird der Text erstellt bzw. vorausgesagt und im oberen Teil des Fensters angezeigt. Zum Beenden oder Starten der Texteingabe klicken Sie einmal mit dem Pen auf die Anzeige. Die Zoom-Geschwindigkeit können Sie unten im Fenster einstellen.

Abbildung 16.4 *Bearbeiten von Text mit Dasher*



Das Konzept von Dasher funktioniert in vielen Sprachen. Weitere Informationen finden Sie auf der Website von Dasher, auf der Sie eine umfassende Dokumentation, Demonstrationen und Schulungsdokumente vorfinden. Die Adresse der Website lautet `http://www.inference.phy.cam.ac.uk/dasher/`

16.7 Fehlersuche

Die virtuelle Tastatur wird im Anmeldefenster nicht angezeigt

Gelegentlich wird die virtuelle Tastatur im Anmeldefenster nicht angezeigt. Zur Behebung dieses Problems starten Sie X Server durch Drücken von Strg + Alt + <— neu bzw. drücken Sie die entsprechende Taste auf Ihrem Tablet PC (falls Sie ein schlankes Modell ohne integrierte Tastatur verwenden). Wenn sich das Problem dadurch nicht beheben lässt, schließen Sie eine externe Tastatur an Ihr Modell an und melden Sie sich über diese Tastatur an.

Die Ausrichtung des Wacom-Grafiktabletts wird nicht geändert

Mit dem Kommando `xrandr` können Sie die Ausrichtung der Ansicht über eine Shell ändern. Geben Sie `xrandr --help` ein, um die verfügbaren Optionen dieses Kommandos anzuzeigen. Wenn Sie gleichzeitig die Ausrichtung des Grafiktabletts ändern möchten, müssen Sie das Kommando wie folgt eingeben:

- Normale Ausrichtung (Drehung um 0°):

```
xrandr --output LVDS ---rotate normal && xsetwacom set "Mouse[7]" Rotate
 NONE
```

- Drehung um 90° (im Uhrzeigersinn, Hochformat):

```
xrandr --output LVDS ---rotate right && xsetwacom set "Mouse[7]" Rotate
 CW
```

- Drehung um 180° (Querformat):

```
 xrandr --output LVDS --rotate inverted && xsetwacom set "Mouse[7]"
Rotate HALF
```

- Drehung um 270° (gegen den Uhrzeigersinn, Hochformat):

```
 xrandr --output LVDS --rotate left && xsetwacom set "Mouse[7]" Rotate
CCW
```

Allerdings wirken sich auf diese Kommandos auch die Einstellungen der Konfigurationsdatei `/etc/X11/xorg.conf` aus. Wenn Sie Ihr Gerät wie unter Abschnitt 16.2, „Konfigurieren des Tablet-Geräts“ (S. 207) beschrieben mit SaX2 konfiguriert haben, sollten die Kommandos wie angegeben funktionieren. Wenn Sie den Parameter `Identifier` des Tablet Stylus-Eingabegeräts in der Datei `xorg.conf` manuell geändert haben, müssen Sie `"Mouse[7]"` durch den neuen `Identifier` ersetzen. Wenn Sie über ein Wacom-Gerät mit Touch-Unterstützung verfügen (Sie können den Cursor auf dem Tablett mit Ihren Fingern verschieben), müssen Sie das Touch-Gerät auch drehen.

16.8 Weiterführende Informationen

Einige der beschriebenen Anwendungen verfügen über keine integrierte Online-Hilfe. Informationen über deren Verwendung und Konfiguration finden Sie jedoch auf dem installierten System unter `/usr/share/doc/package/`*`Paketname`* bzw. im Web:

- Das Xournal-Handbuch finden Sie unter `http://xournal.sourceforge.net/manual.html`
- Die Jarnal-Dokumentation finden Sie unter `http://www.dklevine.com/general/software/tc1000/jarnal.htm#documentation`
- Die man-Seite zu xstroke finden Sie unter `http://davesource.com/Projects/xstroke/xstroke.txt`
- Eine HOWTO-Anleitung zur Konfiguration von X finden Sie auf der Linux Wacom-Website unter `http://linuxwacom.sourceforge.net/index.php/howto/x11`
- Eine überaus informative Website zum Dasher-Projekt finden Sie unter `http://www.inference.phy.cam.ac.uk/dasher/`
- Weitere Informationen und Dokumentation zu CellWriter finden Sie unter `http://risujin.org/cellwriter/`
- Informationen zu gnome-display-properties finden Sie in `http://en.opensuse.org/GNOME/Multiscreen`.

Teil IV. Services

17 Grundlegendes zu Netzwerken

Linux stellt die erforderlichen Netzwerkwerkzeuge und -funktionen für die Integration in alle Arten von Netzwerkstrukturen zur Verfügung. Das üblicherweise von Linux verwendete Protokoll, TCP/IP, verfügt über unterschiedliche Dienste und Sonderfunktionen, die im Folgenden beschrieben werden. Der Netzwerkzugriff über eine Netzwerkkarte, ein Modem oder ein anderes Gerät kann mit YaST konfiguriert werden. Die manuelle Konfiguration ist ebenfalls möglich. In diesem Kapitel werden nur die grundlegenden Mechanismen und die relevanten Netzwerkkonfigurationsdateien behandelt.

Linux und andere Unix-Betriebssysteme verwenden das TCP/IP-Protokoll. Hierbei handelt es sich nicht um ein einzelnes Netzwerkprotokoll, sondern um eine Familie von Netzwerkprotokollen, die unterschiedliche Dienste zur Verfügung stellen. Die in Tabelle 17.1, „Verschiedene Protokolle aus der TCP/IP-Familie“ (S. 222) aufgelisteten Protokolle dienen dem Datenaustausch zwischen zwei Computern über TCP/IP. Über TCP/IP verbundene Netzwerke bilden zusammen ein weltweites Netzwerk, das auch als "das Internet" bezeichnet wird.

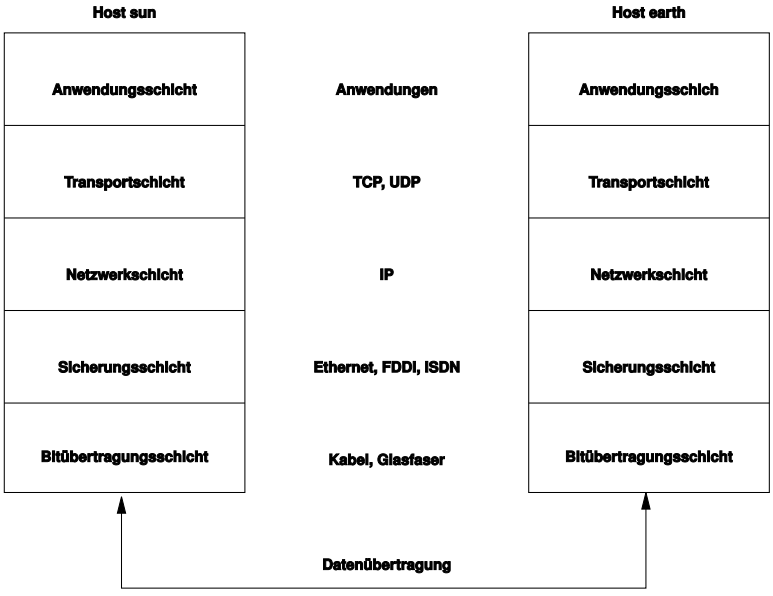
RFC steht für *Request for Comments*. RFCs sind Dokumente, die unterschiedliche Internetprotokolle und Implementierungsverfahren für das Betriebssystem und seine Anwendungen beschreiben. Die RFC-Dokumente beschreiben das Einrichten der Internetprotokolle. Weitere Informationen zu diesen Protokollen finden Sie in den entsprechenden RFC-Dokumenten. Diese sind verfügbar unter `http://www.ietf.org/rfc.html`.

Tabelle 17.1 *Verschiedene Protokolle aus der TCP/IP-Familie*

Protokoll	Beschreibung
TCP	Transmission Control Protocol: Ein verbindungsorientiertes sicheres Protokoll. Die zu übertragenden Daten werden zuerst von der Anwendung als Datenstrom gesendet und vom Betriebssystem in das passende Format konvertiert. Die entsprechende Anwendung auf dem Zielhost empfängt die Daten im ursprünglichen Datenstromformat, in dem sie anfänglich gesendet wurden. TCP ermittelt, ob bei der Übertragung Daten verloren gegangen sind oder die Reihenfolge der Daten durcheinandergeraten ist. TCP wird immer dann implementiert, wenn die Datensequenz eine Rolle spielt.
UDP	User Datagram Protocol: Ein verbindungsloses, nicht sicheres Protokoll. Die zu übertragenden Daten werden in Form von anwendungsseitig generierten Paketen gesendet. Es ist nicht garantiert, in welcher Reihenfolge die Daten beim Empfänger eingehen, und ein Datenverlust ist immer möglich. UDP ist geeignet für datensatzorientierte Anwendungen. Es verfügt über eine kürzere Latenzzeit als TCP.
ICMP	Internet Control Message Protocol: Dies ist im Wesentlichen kein Protokoll für den Endbenutzer, sondern ein spezielles Steuerungsprotokoll, das Fehlerberichte ausgibt und das Verhalten von Computern, die am TCP/IP-Datentransfer teilnehmen, steuern kann. Außerdem bietet es einen speziellen Echomodus, der mit dem Programm "ping" angezeigt werden kann.
IGMP	Internet Group Management Protocol: Dieses Protokoll kontrolliert das Verhalten des Rechners beim Implementieren von IP Multicast.

Der Datenaustausch findet wie in Abbildung 17.1, „Vereinfachtes Schichtmodell für TCP/IP“ (S. 223) dargestellt in unterschiedlichen Schichten statt. Die eigentliche Netzwerkschicht ist der unsichere Datentransfer über IP (Internet Protocol). Oberhalb von IP gewährleistet TCP (Transmission Control Protocol) bis zu einem gewissen Grad die Sicherheit des Datentransfers. Die IP-Schicht wird vom zugrunde liegenden Hardwareabhängigen Protokoll, z. B. Ethernet, unterstützt.

Abbildung 17.1 *Vereinfachtes Schichtmodell für TCP/IP*



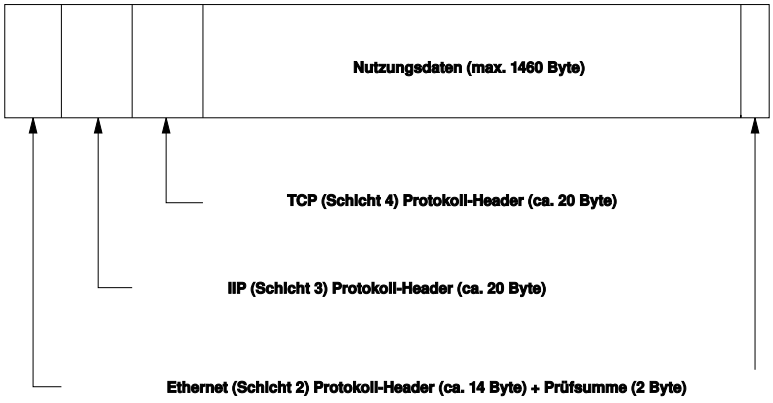
Dieses Diagramm bietet für jede Schicht ein oder zwei Beispiele. Die Schichten sind nach *Abstraktionsstufen* sortiert. Die unterste Schicht ist sehr Hardware-nah. Die oberste Schicht ist beinahe vollständig von der Hardware losgelöst. Jede Schicht hat ihre eigene spezielle Funktion. Die speziellen Funktionen der einzelnen Schichten gehen bereits aus ihrer Bezeichnung hervor. Die Datenverbindungs- und die physische Schicht repräsentieren das verwendete physische Netzwerk, z. B. das Ethernet.

Fast alle Hardwareprotokolle arbeiten auf einer paketorientierten Basis. Die zu übertragenden Daten werden in *Pakete* unterteilt, da sie nicht alle auf einmal gesendet werden können. Die maximale Größe eines TCP/IP-Pakets beträgt ca. 64 KB. Die Pakete sind in der Regel jedoch sehr viel kleiner, da die Netzwerkhardware ein einschränkender Faktor sein kann. Die maximale Größe eines Datenpakets in einem Ethernet beträgt ca. 1500 Byte. Die Größe eines TCP/IP-Pakets ist auf diesen Wert begrenzt, wenn die Daten über ein Ethernet gesendet werden. Wenn mehr Daten übertragen werden, müssen vom Betriebssystem mehr Datenpakete gesendet werden.

Damit die Schichten ihre vorgesehenen Funktionen erfüllen können, müssen im Datenpaket zusätzliche Informationen über die einzelnen Schichten gespeichert sein. Diese Informationen werden im *Header* des Pakets gespeichert. Jede Schicht stellt jedem ausgehenden Paket einen kleinen Datenblock voran, den so genannten Protokoll-

Header. Ein Beispiel für ein TCP/IP-Datenpaket, das über ein Ethernetkabel gesendet wird, ist in Abbildung 17.2, „TCP/IP-Ethernet-Paket“ (S. 224) dargestellt. Die Prüfsumme befindet sich am Ende des Pakets, nicht am Anfang. Dies erleichtert die Arbeit für die Netzwerkhardware.

Abbildung 17.2 *TCP/IP-Ethernet-Paket*


Nutzungsdaten (max. 1460 Byte)
TCP (Schicht 4) Protokoll-Header (ca. 20 Byte)
IIP (Schicht 3) Protokoll-Header (ca. 20 Byte)
Ethernet (Schicht 2) Protokoll-Header (ca. 14 Byte) + Prüfsumme (2 Byte)

Wenn eine Anwendung Daten über das Netzwerk sendet, werden diese Daten durch alle Schichten geleitet, die mit Ausnahme der physischen Schicht alle im Linux-Kernel implementiert sind. Jede Schicht ist für das Vorbereiten der Daten zur Weitergabe an die nächste Schicht verantwortlich. Die unterste Schicht ist letztendlich für das Senden der Daten verantwortlich. Bei eingehenden Daten erfolgt die gesamte Prozedur in umgekehrter Reihenfolge. Die Protokoll-Header werden von den transportierten Daten in den einzelnen Schichten wie die Schalen einer Zwiebel entfernt. Die Transportschicht ist schließlich dafür verantwortlich, die Daten den Anwendungen am Ziel zur Verfügung zu stellen. Auf diese Weise kommuniziert eine Schicht nur mit der direkt darüber bzw. darunter liegenden Schicht. Für Anwendungen ist es irrelevant, ob die Daten über ein 100 MBit/s schnelles FDDI-Netzwerk oder über eine 56-KBit/s-Modemleitung übertragen werden. Ähnlich spielt es für die Datenverbindung keine Rolle, welche Art von Daten übertragen wird, solange die Pakete das richtige Format haben.

17.1 IP-Adressen und Routing

Die in diesem Abschnitt enthaltenen Informationen beziehen sich nur auf IPv4-Netzwerke. Informationen zum IPv6-Protokoll, dem Nachfolger von IPv4, finden Sie in Abschnitt 17.2, „IPv6 – Das Internet der nächsten Generation“ (S. 228).

17.1.1 IP-Adressen

Jeder Computer im Internet verfügt über eine eindeutige 32-Bit-Adresse. Diese 32 Bit (oder 4 Byte) werden in der Regel wie in der zweiten Zeile in Beispiel 17.1, „IP-Adressen schreiben“ (S. 225) dargestellt geschrieben.

Beispiel 17.1 *IP-Adressen schreiben*

```
IP Address (binary):  11000000 10101000 00000000 00010100
IP Address (decimal):      192.     168.       0.      20
```

Im Dezimalformat werden die vier Byte in Dezimalzahlen geschrieben und durch Punkte getrennt. Die IP-Adresse wird einem Host oder einer Netzwerkschnittstelle zugewiesen. Diese Adresse kann weltweit nur einmal verwendet werden. Es gibt zwar Ausnahmen zu dieser Regel, diese sind jedoch für die folgenden Abschnitte nicht relevant.

Die Punkte in IP-Adressen geben das hierarchische System an. Bis in die 1990er-Jahre wurden IP-Adressen strikt in Klassen organisiert. Dieses System erwies sich jedoch als zu wenig flexibel und wurde eingestellt. Heute wird das *klassenlose Routing* (CIDR, Classless Interdomain Routing) verwendet.

17.1.2 Netzmasken und Routing

Mit Netzmasken werden Adressräume eines Subnetzes definiert. Wenn sich zwei Hosts im selben Subnetz befinden, können sie direkt kommunizieren. Anderenfalls benötigen sie die Adresse eines Gateways, das den gesamten Verkehr zwischen dem Subnetz und dem Rest der Welt handhabt. Um zu prüfen, ob sich zwei IP-Adressen im selben Subnetz befinden, wird jede Adresse bitweise mit der Netzmaske "UND"-verknüpft. Sind die Ergebnisse identisch, befinden sich beide IP-Adressen im selben lokalen Netzwerk. Wenn unterschiedliche Ergebnisse ausgegeben werden, kann die entfernte IP-Adresse, und somit die entfernte Schnittstelle, nur über ein Gateway erreicht werden.

Weitere Informationen zur Funktionsweise von Netzmasken finden Sie in Beispiel 17.2, „Verknüpfung von IP-Adressen mit der Netzmaske“ (S. 226). Die Netzmaske besteht aus 32 Bit, die festlegen, welcher Teil einer IP-Adresse zum Netzwerk gehört. Alle Bits mit dem Wert `1` kennzeichnen das entsprechende Bit in der IP-Adresse als zum Netzwerk gehörend. Alle Bits mit dem Wert `0` kennzeichnen Bits innerhalb des Subnetzes. Das bedeutet, je mehr Bits den Wert `1` haben, desto kleiner ist das Netzwerk. Da die Netz-

maske immer aus mehreren aufeinander folgenden Bits mit dem Wert `1` besteht, ist es auch möglich, einfach die Anzahl der Bits in der Netzmaske zu zählen. In Beispiel 17.2, „Verknüpfung von IP-Adressen mit der Netzmaske“ (S. 226) könnte das erste Netz mit 24 Bit auch als `192.168.0.0/24` geschrieben werden.

Beispiel 17.2 *Verknüpfung von IP-Adressen mit der Netzmaske*

```
IP address (192.168.0.20):  11000000 10101000 00000000 00010100
Netmask   (255.255.255.0):  11111111 11111111 11111111 00000000
----------------------------------------------------------------
Result of the link:         11000000 10101000 00000000 00000000
In the decimal system:           192.     168.       0.       0

IP address (213.95.15.200): 11010101 10111111 00001111 11001000
Netmask    (255.255.255.0): 11111111 11111111 11111111 00000000
----------------------------------------------------------------
Result of the link:         11010101 10111111 00001111 00000000
In the decimal system:           213.      95.      15.       0
```

Ein weiteres Beispiel: Alle Computer, die über dasselbe Ethernetkabel angeschlossen sind, befinden sich in der Regel im selben Subnetz und sind direkt zugreifbar. Selbst wenn das Subnetz physisch durch Switches oder Bridges unterteilt ist, können diese Hosts weiter direkt erreicht werden.

IP-Adressen außerhalb des lokalen Subnetzes können nur erreicht werden, wenn für das Zielnetzwerk ein Gateway konfiguriert ist. In den meisten Fällen wird der gesamte externe Verkehr über lediglich ein Gateway gehandhabt. Es ist jedoch auch möglich, für unterschiedliche Subnetze mehrere Gateways zu konfigurieren.

Wenn ein Gateway konfiguriert wurde, werden alle externen IP-Pakete an das entsprechende Gateway gesendet. Dieses Gateway versucht anschließend, die Pakete auf dieselbe Weise (von Host zu Host) weiterzuleiten, bis sie den Zielhost erreicht haben oder ihre TTL-Zeit (Time to Live) abgelaufen ist.

Tabelle 17.2 *Spezifische Adressen*

Adresstyp	Beschreibung
Netzwerkbasis-adresse	Dies ist die Netzmaske, die durch UND mit einer Netzwerkadresse verknüpft ist, wie in Beispiel 17.2, „Verknüpfung von IP-Adressen mit der Netzmaske“ (S. 226) unter `Ergebnis` dargestellt. Diese Adresse kann keinem Host zugewiesen werden.

Adresstyp	Beschreibung
Broadcast-Adresse	Dies bedeutet im Wesentlichen "Senden an alle Hosts in diesem Subnetz." Um die Broadcast-Adresse zu generieren, wird die Netzmaske in die binäre Form invertiert und mit einem logischen ODER mit der Netzwerkbasisadresse verknüpft. Das obige Beispiel ergibt daher die Adresse 192.168.0.255. Diese Adresse kann keinem Host zugeordnet werden.
Lokaler Host	Die Adresse `127.0.0.1` ist auf jedem Host dem "Loopback-Device" zugewiesen. Mit dieser Adresse kann eine Verbindung zu Ihrem Computer hergestellt werden.

Da IP-Adressen weltweit eindeutig sein müssen, können Sie nicht einfach eine Adresse nach dem Zufallsprinzip wählen. Zum Einrichten eines privaten IP-basierten Netzwerks stehen drei Adressdomänen zur Verfügung. Diese können keine Verbindung zum Internet herstellen, da sie nicht über das Internet übertragen werden können. Diese Adressdomänen sind in RFC 1597 festgelegt und werden in Tabelle 17.3, „Private IP-Adressdomänen“ (S. 227) aufgelistet.

Tabelle 17.3 *Private IP-Adressdomänen*

Netzwerk/Netzmaske	Domäne
`10.0.0.0/255.0.0.0`	`10.x.x.x`
`172.16.0.0/255.240.0.0`	`172.16.x.x – 172.31.x.x`
`192.168.0.0/255.255.0.0`	`192.168.x.x`

17.2 IPv6 – Das Internet der nächsten Generation

WICHTIG: IBM-System z: IPv6-Unterstützung

IPv6 wird von den CTC- und IUCV-Netzwerkverbindungen der IBM-System z-Hardware nicht unterstützt.

Aufgrund der Entstehung des WWW (World Wide Web) hat das Internet in den letzten 15 Jahren ein explosives Wachstum mit einer immer größer werdenden Anzahl von Computern erfahren, die über TCP/IP kommunizieren. Seit Tim Berners-Lee bei CERN (`http://public.web.cern.ch`) 1990 das WWW erfunden hat, ist die Anzahl der Internethosts von ein paar tausend auf ca. 100 Millionen angewachsen.

Wie bereits erwähnt, besteht eine IPv4-Adresse nur aus 32 Bit. Außerdem gehen zahlreiche IP-Adressen verloren, da sie aufgrund die Organisation der Netzwerke nicht verwendet werden können. Die Anzahl der in Ihrem Subnetz verfügbaren Adressen ist zwei hoch der Anzahl der Bits minus zwei. Ein Subnetz verfügt also beispielsweise über 2, 6 oder 14 Adressen. Um beispielsweise 128 Hosts mit dem Internet zu verbinden, benötigen Sie ein Subnetz mit 256 IP-Adressen, von denen nur 254 verwendbar sind, da zwei IP-Adressen für die Struktur des Subnetzes selbst benötigt werden: die Broadcast- und die Basisnetzwerkadresse.

Unter dem aktuellen IPv4-Protokoll sind DHCP oder NAT (Network Address Translation) die typischen Mechanismen, um einem potenziellen Adressmangel vorzubeugen. Kombiniert mit der Konvention, private und öffentliche Adressräume getrennt zu halten, können diese Methoden den Adressmangel sicherlich mäßigen. Das Problem liegt in der Konfiguration der Adressen, die schwierig einzurichten und zu verwalten ist. Um einen Host in einem IPv4-Netzwerk einzurichten, benötigen Sie mehrere Adressen, z. B. die IP-Adresse des Hosts, die Subnetzmaske, die Gateway-Adresse und möglicherweise die Adresse des Namenservers. Alle diese Einträge müssen bekannt sein und können nicht von anderer Stelle her abgeleitet werden.

Mit IPv6 gehören sowohl der Adressmangel als auch die komplizierte Konfiguration der Vergangenheit an. Die folgenden Abschnitte enthalten weitere Informationen zu den Verbesserungen und Vorteilen von IPv6 sowie zum Übergang vom alten zum neuen Protokoll.

17.2.1 Vorteile

Die wichtigste und augenfälligste Verbesserung durch das neue Protokoll ist der enorme Zuwachs des verfügbaren Adressraums. Eine IPv6-Adresse besteht aus 128-Bit-Werten und nicht aus den herkömmlichen 32 Bit. Dies ermöglicht mehrere Billiarden IP-Adressen.

IPv6-Adressen unterscheiden sich nicht nur hinsichtlich ihrer Länge gänzlich von ihren Vorgängern. Sie verfügen auch über eine andere interne Struktur, die spezifischere Informationen zu den Systemen und Netzwerken enthalten kann, zu denen sie gehören. Weitere Informationen hierzu finden Sie in Abschnitt 17.2.2, „Adresstypen und -struktur“ (S. 230).

In der folgenden Liste werden einige der wichtigsten Vorteile des neuen Protokolls aufgeführt:

Automatische Konfiguration
: IPv6 macht das Netzwerk "Plug-and-Play"-fähig, d. h., ein neu eingerichtetes System wird ohne jegliche manuelle Konfiguration in das (lokale) Netzwerk integriert. Der neue Host verwendet die automatischen Konfigurationsmechanismen, um seine eigene Adresse aus den Informationen abzuleiten, die von den benachbarten Routern zur Verfügung gestellt werden. Dabei nutzt er ein Protokoll, das als *ND-Protokoll* (Neighbor Discovery) bezeichnet wird. Diese Methode erfordert kein Eingreifen des Administrators und für die Adresszuordnung muss kein zentraler Server verfügbar sein. Dies ist ein weiterer Vorteil gegenüber IPv4, bei dem für die automatische Adresszuordnung ein DHCP-Server erforderlich ist.

Mobilität
: IPv6 ermöglicht es, einer Netzwerkschnittstelle gleichzeitig mehrere Adressen zuzuordnen. Benutzer können daher einfach auf mehrere Netzwerke zugreifen. Dies lässt sich mit den internationalen Roaming-Diensten vergleichen, die von Mobilfunkunternehmen angeboten werden: Wenn Sie das Mobilfunkgerät ins Ausland mitnehmen, meldet sich das Telefon automatisch bei einem ausländischen Dienst an, der sich im entsprechenden Bereich befindet. Sie können also überall unter der gleichen Nummer erreicht werden und können telefonieren als wären Sie zu Hause.

Sichere Kommunikation
: Bei IPv4 ist die Netzwerksicherheit eine Zusatzfunktion. IPv6 umfasst IPSec als eine seiner Kernfunktionen und ermöglicht es Systemen, über einen sicheren Tunnel

zu kommunizieren, um das Ausspionieren durch Außenstehende über das Internet zu verhindern.

Abwärtskompatibilität
: Realistisch gesehen, ist es unmöglich, das gesamte Internet auf einmal von IPv4 auf IPv6 umzustellen. Daher ist es wichtig, dass beide Protokolle nicht nur im Internet, sondern auf einem System koexistieren können. Dies wird durch kompatible Adressen (IPv4-Adressen können problemlos in IPv6-Adressen konvertiert werden) und die Verwendung von Tunnels gewährleistet. Weitere Informationen hierzu finden Sie unter Abschnitt 17.2.3, „Koexistenz von IPv4 und IPv6“ (S. 235). Außerdem können Systeme eine *Dual-Stack-IP*-Technik verwenden, um beide Protokolle gleichzeitig unterstützen zu können. Dies bedeutet, dass sie über zwei Netzwerk-Stacks verfügen, die vollständig unabhängig voneinander sind, sodass zwischen den beiden Protokollversionen keine Konflikte auftreten.

Bedarfsgerechte Dienste über Multicasting
: Mit IPv4 müssen einige Dienste, z. B. SMB, ihre Pakete via Broadcast an alle Hosts im lokalen Netzwerk verteilen. IPv6 ermöglicht einen sehr viel ausgefeilterten Ansatz. Server können Hosts über *Multicasting* ansprechen, d. h. sie sprechen mehrere Hosts als Teile einer Gruppe an (im Gegensatz zur Adressierung aller Hosts über *Broadcasting* oder der Einzeladressierung der Hosts über *Unicasting*). Welche Hosts als Gruppe adressiert werden, kann je nach Anwendung unterschiedlich sein. Es gibt einige vordefinierte Gruppen, mit der beispielsweise alle Namenserver (die *Multicast-Gruppe "all name servers"*) oder alle Router (die *Multicast-Gruppe "all routers"*) angesprochen werden können.

17.2.2 Adresstypen und -struktur

Wie bereits erwähnt hat das aktuelle IP-Protokoll zwei wichtige Nachteile: Es stehen zunehmend weniger IP-Adressen zur Verfügung und das Konfigurieren des Netzwerks und Verwalten der Routing-Tabellen wird komplexer und aufwändiger. IPv6 löst das erste Problem durch die Erweiterung des Adressraums auf 128 Bit. Das zweite Problem wird durch die Einführung einer hierarchischen Adressstruktur behoben, die mit weiteren hoch entwickelten Techniken zum Zuordnen von Netzwerkadressen sowie mit dem *Multihoming* (der Fähigkeit, einem Gerät mehrere Adressen zuzuordnen und so den Zugriff auf mehrere Netzwerke zu ermöglichen) kombiniert wird.

Bei der Arbeit mit IPv6 ist es hilfreich, die drei unterschiedlichen Adresstypen zu kennen:

Unicast
: Adressen dieses Typs werden genau einer Netzwerkschnittstelle zugeordnet. Pakete mit derartigen Adressen werden nur einem Ziel zugestellt. Unicast-Adressen werden dementsprechend zum Übertragen von Paketen an einzelne Hosts im lokalen Netzwerk oder im Internet verwendet.

Multicast
: Adressen dieses Typs beziehen sich auf eine Gruppe von Netzwerkschnittstellen. Pakete mit derartigen Adressen werden an alle Ziele zugestellt, die dieser Gruppe angehören. Multicast-Adressen werden hauptsächlich von bestimmten Netzwerkdiensten für die Kommunikation mit bestimmten Hostgruppen verwendet, wobei diese gezielt adressiert werden.

Anycast
: Adressen dieses Typs beziehen sich auf eine Gruppe von Schnittstellen. Pakete mit einer derartigen Adresse werden gemäß den Prinzipien des zugrunde liegenden Routing-Protokolls dem Mitglied der Gruppe gesendet, das dem Absender am nächsten ist. Anycast-Adressen werden verwendet, damit Hosts Informationen zu Servern schneller abrufen können, die im angegebenen Netzwerkbereich bestimmte Dienste anbieten. Sämtliche Server desselben Typs verfügen über dieselbe Anycast-Adresse. Wann immer ein Host einen Dienst anfordert, erhält er eine Antwort von dem vom Routing-Protokoll ermittelten nächstgelegenen Server. Wenn dieser Server aus irgendeinem Grund nicht erreichbar ist, wählt das Protokoll automatisch den zweitnächsten Server, dann den dritten usw. aus.

Eine IPv6-Adresse besteht aus acht vierstelligen Feldern, wobei jedes 16 Bit repräsentiert, und wird in hexadezimaler Notation geschrieben. Die Felder werden ebenfalls durch Doppelpunkte (`:`) getrennt. Alle führenden Null-Byte innerhalb eines bestimmten Felds können ausgelassen werden, alle anderen Nullen jedoch nicht. Eine weitere Konvention ist, dass mehr als vier aufeinander folgenden Null-Byte mit einem doppelten Doppelpunkt zusammengefasst werden können. Jedoch ist pro Adresse nur ein solcher doppelter Doppelpunkt (`::`) zulässig. Diese Art der Kurznotation wird in Beispiel 17.3, „Beispiel einer IPv6-Adresse“ (S. 231) dargestellt, in dem alle drei Zeilen derselben Adresse entsprechen.

Beispiel 17.3 *Beispiel einer IPv6-Adresse*

```
fe80 : 0000 : 0000 : 0000 : 0000 : 10 : 1000 : 1a4
fe80 :    0 :    0 :    0 :    0 : 10 : 1000 : 1a4
fe80 :                            : 10 : 1000 : 1a4
```

Jeder Teil einer IPv6-Adresse hat eine festgelegte Funktion. Die ersten Byte bilden das Präfix und geben den Typ der Adresse an. Der mittlere Teil ist der Netzwerkteil der Adresse, der möglicherweise nicht verwendet wird. Das Ende der Adresse bildet der Hostteil. Bei IPv6 wird die Netzmaske definiert, indem die Länge des Präfixes nach einem Schrägstrich am Ende der Adresse angegeben wird. Adressen wie in Beispiel 17.4, „IPv6-Adressen mit Angabe der Präfix-Länge“ (S. 232) enthalten Informationen zum Netzwerk (die ersten 64 Bit) und zum Hostteil (die letzten 64 Bit). Die `64` bedeutet, dass die Netzmaske mit 64 1-Bit-Werten von links gefüllt wird. Wie bei IPv4 wird die IP-Adresse mit den Werten aus der Netzmaske durch UND verknüpft, um zu ermitteln, ob sich der Host im selben oder einem anderen Subnetz befindet.

Beispiel 17.4 *IPv6-Adressen mit Angabe der Präfix-Länge*

```
fe80::10:1000:1a4/64
```

IPv6 kennt mehrere vordefinierte Präfixtypen. Einige von diesen sind in Tabelle 17.4, „Unterschiedliche IPv6-Präfixe“ (S. 232) aufgeführt.

Tabelle 17.4 *Unterschiedliche IPv6-Präfixe*

Präfix (hexadezimal)	Definition
`00`	IPv4-über-IPv6-Kompatibilitätsadressen. Diese werden zur Erhaltung der Kompatibilität mit IPv4 verwendet. Für diesen Adresstyp wird ein Router benötigt, der IPv6-Pakete in IPv4-Pakete konvertieren kann. Mehrere spezielle Adressen, z. B. die für das Loopback-Device, verfügen ebenfalls über dieses Präfix.
`2` oder `3` als erste Stelle	Aggregierbare globale Unicast-Adressen. Wie bei IPv4 kann eine Schnittstelle zugewiesen werden, um einen Teil eines bestimmten Subnetzes zu bilden. Aktuell stehen die folgenden Adressräume zur Verfügung: `2001::/16` (Adressraum Produktionsqualität) und `2002::/16` (6to4-Adressraum).
`fe80::/10`	Link-local-Adressen. Adressen mit diesem Präfix dürfen nicht geroutet werden und können daher nur im gleichen Subnetz erreicht werden.

Präfix (hexadezimal)	Definition
`fec0::/10`	Site-local-Adressen. Diese Adressen dürfen zwar geroutet werden, aber nur innerhalb des Organisationsnetzwerks, dem sie angehören. Damit entsprechen diese Adressen den bisherigen privaten Netzen (beispielsweise `10.x.x.x`).
`ff`	Dies sind Multicast-Adressen.

Eine Unicast-Adresse besteht aus drei grundlegenden Komponenten:

Öffentliche Topologie
: Der erste Teil, der unter anderem auch eines der oben erwähnten Präfixe enthält, dient dem Routing des Pakets im öffentlichen Internet. Hier sind Informationen zum Provider oder der Institution kodiert, die den Netzwerkzugang bereitstellen.

Site-Topologie
: Der zweite Teil enthält Routing-Informationen zum Subnetz, in dem das Paket zugestellt werden soll.

Schnittstellen-ID
: Der dritte Teil identifiziert eindeutig die Schnittstelle, an die das Paket gerichtet ist. Dies erlaubt, die MAC-Adresse als Adressbestandteil zu verwenden. Da diese weltweit nur einmal vorhanden und zugleich vom Hardwarehersteller fest vorgegeben ist, vereinfacht sich die Konfiguration auf diese Weise sehr. Die ersten 64 Bit werden zu einem so genannten `EUI-64`-Token zusammengefasst. Dabei werden die letzten 48 Bit der MAC-Adresse entnommen und die restlichen 24 Bit enthalten spezielle Informationen, die etwas über den Typ des Tokens aussagen. Das ermöglicht dann auch, Geräten ohne MAC-Adresse (z. B. PPP- und ISDN-Verbindungen) ein `EUI-64`-Token zuzuweisen.

Abgeleitet aus diesem Grundaufbau werden bei IPv6 fünf verschiedene Typen von Unicast-Adressen unterschieden:

`::` (nicht spezifiziert)
: Ein Host verwendet diese Adresse als Quelladresse, wenn seine Netzwerkschnittstelle zum ersten Mal initialisiert wird und die Adresse noch nicht anderweitig ermittelt werden kann.

`::1` (Loopback)
: Adresse des Loopback-Device.

IPv4-kompatible Adressen
: Die IPv6-Adresse setzt sich aus der IPv4-Adresse und einem Präfix von 96 0-Bits zusammen. Dieser Typ der Kompatibilitätsadresse wird beim Tunneling verwendet (siehe Abschnitt 17.2.3, „Koexistenz von IPv4 und IPv6“ (S. 235)). IPv4/IPv6-Hosts können so mit anderen kommunizieren, die sich in einer reinen IPv4-Umgebung befinden.

IPv6-gemappte IPv4-Adressen
: Dieser Adresstyp gibt die Adresse in IPv6-Notation an.

Lokale Adressen
: Es gibt zwei Typen von Adressen zum rein lokalen Gebrauch:

  link-local
  : Dieser Adresstyp ist ausschließlich für den Gebrauch im lokalen Subnetz bestimmt. Router dürfen Pakete mit solcher Ziel- oder Quelladresse nicht an das Internet oder andere Subnetze weiterreichen. Diese Adressen zeichnen sich durch ein spezielles Präfix (`fe80::/10`) und die Schnittstellen-ID der Netzwerkkarte aus. Der Mittelteil der Adresse besteht aus Null-Bytes. Diese Art Adresse wird von den Autokonfigurationsmethoden verwendet, um Hosts im selben Subnetz anzusprechen.

  site-local
  : Pakete mit diesem Adresstyp dürfen zwischen einzelnen Subnetzen geroutet werden, jedoch nicht außerhalb einer Organisation ins Internet gelangen. Solche Adressen werden für Intranets eingesetzt und sind ein Äquivalent zu den privaten IPv4-Adressen. Neben einem definierten Präfix (`fec0::/10`) und der Schnittstellen-ID enthalten diese Adressen ein 16-Bit-Feld, in dem die Subnetz-ID kodiert ist. Der Rest wird wieder mit Null-Bytes aufgefüllt.

Zusätzlich gibt es in IPv6 eine grundsätzlich neue Funktion: Einer Netzwerkschnittstelle werden üblicherweise mehrere IP-Adressen zugewiesen. Das hat den Vorteil, dass mehrere verschiedene Netze zur Verfügung stehen. Eines dieser Netzwerke kann mit der MAC-Adresse und einem bekannten Präfix vollautomatisch konfiguriert werden, sodass sofort nach der Aktivierung von IPv6 alle Hosts im lokalen Netz über Link-local-Adressen erreichbar sind. Durch die MAC-Adresse als Bestandteil der IP-Adresse ist jede dieser Adressen global eindeutig. Einzig die Teile der *Site-Topologie* und der

öffentlichen Topologie können variieren, je nachdem in welchem Netz dieser Host aktuell zu erreichen ist.

Bewegt sich ein Host zwischen mehreren Netzen hin und her, braucht er mindestens zwei Adressen. Die eine, seine *Home-Adresse*, beinhaltet neben der Schnittstellen-ID die Informationen zu dem Heimatnetz, in dem der Computer normalerweise betrieben wird, und das entsprechende Präfix. Die Home-Adresse ist statisch und wird in der Regel nicht verändert. Alle Pakete, die für diesen Host bestimmt sind, werden ihm sowohl im eigenen als auch in fremden Netzen zugestellt. Möglich wird die Zustellung im Fremdnetz über wesentliche Neuerungen des IPv6-Protokolls, z. B. *Stateless Autoconfiguration* und *Neighbor Discovery*. Der mobile Rechner hat neben seiner Home-Adresse eine oder mehrere weitere Adressen, die zu den fremden Netzen gehören, in denen er sich bewegt. Diese Adressen heißen *Care-of*-Adressen. Im Heimatnetz des mobilen Rechners muss eine Instanz vorhanden sein, die an seine Home-Adresse gerichtete Pakete nachsendet, sollte er sich in einem anderen Netz befinden. Diese Funktion wird in einer IPv6-Umgebung vom *Home-Agenten* übernommen. Er stellt alle Pakete, die an die Home-Adresse des mobilen Rechners gerichtet sind, über einen Tunnel zu. Pakete, die als Zieladresse die Care-of-Adresse tragen, können ohne Umweg über den Home-Agenten zugestellt werden.

17.2.3 Koexistenz von IPv4 und IPv6

Die Migration aller mit dem Internet verbundenen Hosts von IPv4 auf IPv6 wird nicht auf einen Schlag geschehen. Vielmehr werden das alte und das neue Protokoll noch eine ganze Weile nebeneinanderher existieren. Die Koexistenz auf einem Rechner ist dann möglich, wenn beide Protokolle im *Dual Stack*-Verfahren implementiert sind. Es bleibt aber die Frage, wie IPv6-Rechner mit IPv4-Rechnern kommunizieren können und wie IPv6-Pakete über die momentan noch vorherrschenden IPv4-Netze transportiert werden sollen. Tunneling und die Verwendung von Kompatibilitätsadressen (siehe Abschnitt 17.2.2, „Adresstypen und -struktur“ (S. 230)) sind hier die besten Lösungen.

IPv6-Hosts, die im (weltweiten) IPv4-Netzwerk mehr oder weniger isoliert sind, können über Tunnel kommunizieren: IPv6-Pakete werden als IPv4-Pakete gekapselt und so durch ein ein IPv4-Netzwerk übertragen. Ein *Tunnel* ist definiert als die Verbindung zwischen zwei IPv4-Endpunkten. Hierbei müssen die Pakete die IPv6-Zieladresse (oder das entsprechende Präfix) und die IPv4-Adresse des entfernten Hosts am Tunnelendpunkt enthalten. Einfache Tunnel können von den Administratoren zwischen ihren Netzwerken manuell und nach Absprache konfiguriert werden. Ein solches Tunneling wird *statisches Tunneling* genannt.

Trotzdem reicht manuelles Tunneling oft nicht aus, um die Menge der zum täglichen vernetzten Arbeiten nötigen Tunnel aufzubauen und zu verwalten. Aus diesem Grund wurden für IPv6 drei verschiedene Verfahren entwickelt, die das *dynamische Tunneling* erlauben:

6over4
: IPv6-Pakete werden automatisch in IPv4-Pakete verpackt und über ein IPv4-Netzwerk versandt, in dem Multicasting aktiviert ist. IPv6 wird vorgespiegelt, das gesamte Netzwerk (Internet) sei ein einziges, riesiges LAN (Local Area Network). So wird der IPv4-Endpunkt des Tunnel automatisch ermittelt. Nachteile dieser Methode sind die schlechte Skalierbarkeit und die Tatsache, dass IP-Multicasting keineswegs im gesamten Internet verfügbar ist. Diese Lösung eignet sich für kleinere Netzwerke, die die Möglichkeit von IP-Multicasting bieten. Die zugrunde liegenden Spezifikationen sind in RFC 2529 enthalten.

6to4
: Bei dieser Methode werden automatisch IPv4-Adressen aus IPv6-Adressen generiert. So können isolierte IPv6-Hosts über ein IPv4-Netz miteinander kommunizieren. Allerdings gibt es einige Probleme, die die Kommunikation zwischen den isolierten IPv6-Hosts und dem Internet betreffen. Diese Methode wird in RFC 3056 beschrieben.

IPv6 Tunnel Broker
: Dieser Ansatz sieht spezielle Server vor, die für IPv6 automatisch dedizierte Tunnel anlegen. Diese Methode wird in RFC 3053 beschrieben.

17.2.4 IPv6 konfigurieren

Um IPv6 zu konfigurieren, müssen Sie auf den einzelnen Arbeitsstationen in der Regel keine Änderungen vornehmen. IPv6 ist standardmäßig aktiviert. Sie können IPv6 während der Installation im Schritt der Netzwerkkonfiguration deaktivieren (siehe „Netzwerkkonfiguration“ (Kapitel 6, *Installation mit YaST*, ↑*Bereitstellungshandbuch*)). Um IPv6 auf einem installierten System zu deaktivieren oder zu aktivieren, verwenden Sie das Modul YaST-*Netzwerkeinstellungen*. Aktivieren oder deaktivieren Sie auf dem Karteireiter *Globale Optionen* die Option *IPv6 aktivieren*, falls nötig. Um IPv6 manuell zu aktivieren, geben Sie `modprobe ipv6` als `root` ein.

Aufgrund des Konzepts der automatischen Konfiguration von IPv6 wird der Netzwerkkarte eine Adresse im *Link-local*-Netzwerk zugewiesen. In der Regel werden Routing-

Tabellen nicht auf Arbeitsstationen verwaltet. Bei Netzwerkroutern kann von der Arbeitsstation unter Verwendung des *Router-Advertisement-Protokolls* abgefragt werden, welches Präfix und welche Gateways implementiert werden sollen. Zum Einrichten eines IPv6-Routers kann das radvd-Programm verwendet werden. Dieses Programm informiert die Arbeitsstationen darüber, welches Präfix und welche Router für die IPv6-Adressen verwendet werden sollen. Alternativ können Sie die Adressen und das Routing auch mit zebra/quagga automatisch konfigurieren.

Weitere Informationen zum Einrichten der unterschiedlichen Tunneltypen mithilfe der Dateien im Verzeichnis `/etc/sysconfig/network` finden Sie auf der man-Seite "ifcfg-tunnel (5)".

17.2.5 Weiterführende Informationen

Das komplexe IPv6-Konzept wird im obigen Überblick nicht vollständig abgedeckt. Weitere ausführliche Informationen zu dem neuen Protokoll finden Sie in den folgenden Online-Dokumentationen und -Büchern:

`http://www.ipv6.org/`
: Alles rund um IPv6.

`http://www.ipv6day.org`
: Alle Informationen, die Sie benötigen, um Ihr eigenes IPv6-Netzwerk zu starten.

`http://www.ipv6-to-standard.org/`
: Die Liste der IPv6-fähigen Produkte.

`http://www.bieringer.de/linux/IPv6/`
: Hier finden Sie den Beitrag "Linux IPv6 HOWTO" und viele verwandte Links zum Thema.

RFC 2640
: Die grundlegenden IPv6-Spezifikationen.

IPv6 Essentials
: Ein Buch, in dem alle wichtigen Aspekte zum Thema enthalten sind, ist *IPv6 Essentials* von Silvia Hagen (ISBN 0-596-00125-8).

17.3 Namensauflösung

Mithilfe von DNS kann eine IP-Adresse einem oder sogar mehreren Namen zugeordnet werden und umgekehrt auch ein Name einer IP-Adresse. Unter Linux erfolgt diese Umwandlung üblicherweise durch eine spezielle Software namens bind. Der Computer, der diese Umwandlung dann erledigt, nennt sich *Namenserver*. Dabei bilden die Namen wieder ein hierarchisches System, in dem die einzelnen Namensbestandteile durch Punkte getrennt sind. Die Namenshierarchie ist aber unabhängig von der oben beschriebenen Hierarchie der IP-Adressen.

Nehmen Sie als Beispiel einen vollständigen Namen wie `jupiter.example.com`, der im Format `hostname.domäne` geschrieben wurde. Ein vollständiger Name, der als *Fully Qualified Domain Name* oder kurz als FQDN bezeichnet wird, besteht aus einem Host- und einem Domänennamen (`example.com`). Ein Bestandteil des Domänennamens ist die *Top Level Domain* oder TLD (`com`).

Aus historischen Gründen ist die Zuteilung der TLDs etwas verwirrend. So werden in den USA traditionell dreibuchstabige TLDs verwendet, woanders aber immer die aus zwei Buchstaben bestehenden ISO-Länderbezeichnungen. Seit 2000 stehen zusätzliche TLDs für spezielle Sachgebiete mit zum Teil mehr als drei Buchstaben zur Verfügung (z. B. `.info`, `.name`, `.museum`).

In der Frühzeit des Internets (vor 1990) gab es die Datei `/etc/hosts`, in der die Namen aller im Internet vertretenen Rechner gespeichert waren. Dies erwies sich bei der schnell wachsenden Menge der mit dem Internet verbundenen Computer als unpraktikabel. Deshalb wurde eine dezentralisierte Datenbank entworfen, die die Hostnamen verteilt speichern kann. Diese Datenbank, eben jener oben erwähnte Namenserver, hält also nicht die Daten aller Computer im Internet vorrätig, sondern kann Anfragen an ihm nachgeschaltete, andere Namenserver weiterdelegieren.

An der Spitze der Hierarchie befinden sich die *Root-Namenserver*. Die root-Namenserver verwalten die Domänen der obersten Ebene (Top Level Domains) und werden vom Network Information Center (NIC) verwaltet. Der Root-Namenserver kennt die jeweils für eine Top Level Domain zuständigen Namenserver. Weitere Informationen zu TLD-NICs finden Sie unter `http://www.internic.net`.

DNS kann noch mehr als nur Hostnamen auflösen. Der Namenserver weiß auch, welcher Host für eine ganze Domäne E-Mails empfängt (der *Mail Exchanger (MX)*).

Damit auch Ihr Rechner einen Namen in eine IP-Adresse auflösen kann, muss ihm mindestens ein Namenserver mit einer IP-Adresse bekannt sein. Die Konfiguration eines Namenservers erledigen Sie komfortabel mithilfe von YaST. Falls Sie eine Einwahl über Modem vornehmen, kann es sein, dass die manuelle Konfiguration eines Namenservers nicht erforderlich ist. Das Einwahlprotokoll liefert die Adresse des Namenservers bei der Einwahl gleich mit. Die Konfiguration des Namenserverzugriffs unter SUSE® Linux Enterprise Server wird unter „Konfigurieren des Hostnamens und DNS“ (S. 250) beschrieben. Eine Beschreibung zum Einrichten Ihres Nameservers finden Sie in Kapitel 21, *Domain Name System (DNS)* (S. 313).

Eng verwandt mit DNS ist das Protokoll `whois`. Mit dem gleichnamigen Programm whois können Sie schnell ermitteln, wer für eine bestimmte Domäne verantwortlich ist.

ANMERKUNG: MDNS- und .local-Domänennamen

Die Domäne `.local` der obersten Stufe wird vom Resolver als link-local-Domäne behandelt. DNS-Anforderungen werden als Multicast-DNS-Anforderungen anstelle von normalen DNS-Anforderungen gesendet. Wenn Sie in Ihrer Nameserver-Konfiguration die Domäne `.local` verwenden, müssen Sie diese Option in `/etc/host.conf` ausschalten. Lesen Sie auch die man-Seite `host.conf`.

Wenn Sie MDNS während der Installation ausschalten möchten, verwenden Sie `nomdns=1` als Boot-Parameter.

Weitere Informationen zum Multicast-DNS finden Sie unter `http://www.multicastdns.org`.

17.4 Konfigurieren von Netzwerkverbindungen mit YaST

Unter Linux gibt es viele unterstützte Netzwerktypen. Die meisten verwenden unterschiedliche Gerätenamen und die Konfigurationsdateien sind im Dateisystem an unterschiedlichen Speicherorten verteilt. Einen detaillierten Überblick über die Aspekte der manuellen Netzwerkkonfiguration finden Sie in Abschnitt 17.6, „Manuelle Netzwerkkonfiguration“ (S. 267).

Auf dem SUSE Linux Enterprise Desktop, auf dem NetworkManager standardmäßig aktiv ist, werden alle Netzwerkkarten konfiguriert. Wenn NetworkManager nicht aktiv ist, wird nur die erste Schnittstelle mit Link-Up (einem angeschlossenen Netzwerkkabel) automatisch konfiguriert. Zusätzliche Hardware kann jederzeit nach Abschluss der Installation auf dem installierten System konfiguriert werden. In den folgenden Abschnitten wird die Netzwerkkonfiguration für alle von SUSE Linux Enterprise Server unterstützten Netzwerkverbindungen beschrieben.

TIPP: IBM-System z: Netzwerkkarten mit Hotplug-Unterstützung

Auf den IBM-System z-Plattformen werden Hotplug-fähige Netzwerkkarten unterstützt, aber nicht deren automatische Netzwerkintegration über DHCP (wie beim PC). Nach der Erkennung muss die Schnittstelle manuell konfiguriert werden.

17.4.1 Konfigurieren der Netzwerkkarte mit YaST

Zur Konfiguration verkabelter oder drahtloser Netzwerkkarten in YaST wählen Sie *Netzwerkgeräte* > *Netzwerkeinstellungen* aus. Nach dem Öffnen des Moduls zeigt YaST das Dialogfeld *Netzwerkeinstellungen* mit den vier Karteireitern *Globale Optionen*, *Übersicht*, *Hostname/DNS* und *Routing* an.

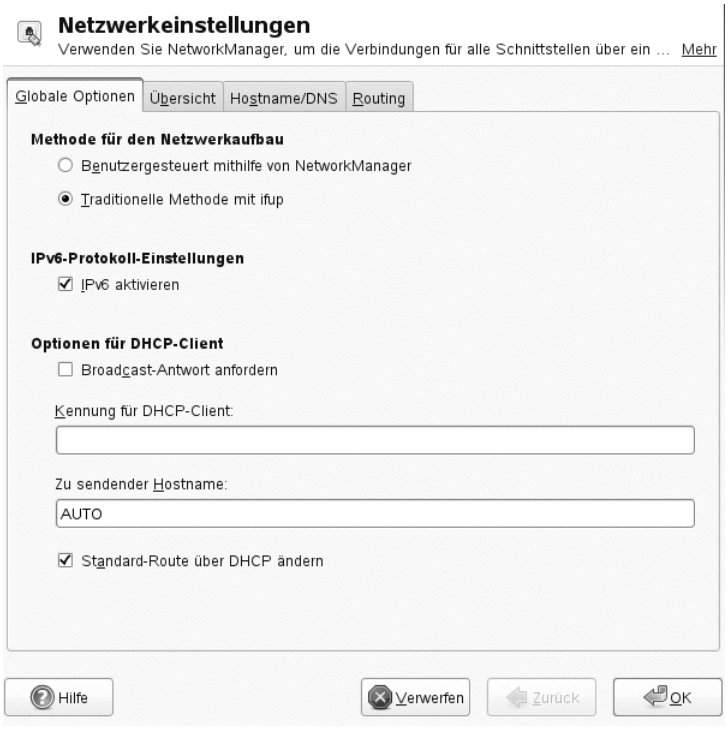
Auf dem Karteireiter *Globale Optionen* können allgemeine Netzwerkoptionen wie die Verwendung der Optionen NetworkManager, IPv6 und global DHCP festgelegt werden. Weitere Informationen finden Sie unter „Konfigurieren globaler Netzwerkoptionen“ (S. 242).

Der Karteireiter *Übersicht* enthält Informationen über installierte Netzwerkschnittstellen und -konfigurationen. Jede korrekt erkannte Netzwerkkarte wird dort mit ihrem Namen aufgelistet. In diesem Dialogfeld können Sie Karten manuell konfigurieren, entfernen oder ihre Konfiguration ändern. Informationen zum manuellen Konfigurieren von Karten, die nicht automatisch erkannt wurden, finden Sie unter „Konfigurieren einer unerkannten Netzwerkkarte“ (S. 249). Informationen zum Ändern der Konfiguration einer bereits konfigurierten Karte finden Sie unter „Ändern der Konfiguration einer Netzwerkkarte“ (S. 243).

Auf dem Karteireiter *Hostname/DNS* können der Hostname des Computers sowie die zu verwendenden Nameserver festgelegt werden. Weitere Informationen finden Sie unter „Konfigurieren des Hostnamens und DNS“ (S. 250).

Der Karteireiter *Routing* wird zur Konfiguration des Routings verwendet. Weitere Informationen finden Sie unter „Konfigurieren des Routing“ (S. 252).

Abbildung 17.3 *Konfigurieren der Netzwerkeinstellungen*



Konfigurieren globaler Netzwerkoptionen

Auf dem Karteireiter *Globale Optionen* des YaST-Moduls *Netzwerkeinstellungen* können wichtige globale Netzwerkoptionen wie die Verwendung der Optionen NetworkManager, IPv6 und DHCP-Client festgelegt werden. Diese Einstellungen sind für alle Netzwerkschnittstellen anwendbar.

Unter *Netzwerkeinrichtungsmethode* wählen Sie die Methode aus, mit der Netzwerkverbindungen verwaltet werden sollen. Wenn die Verbindungen für alle Schnittstellen über das Desktop-Applet NetworkManager verwaltet werden sollen, wählen Sie *Benutzergesteuert mithilfe von NetworkManager* aus. Diese Option eignet sich besonders für den Wechsel zwischen verschiedenen verkabelten und drahtlosen Netzwerken. Wenn Sie keine Desktop-Umgebung (GNOME oder KDE) ausführen oder wenn Ihr Computer ein Xen-Server oder ein virtuelles System ist oder Netzwerkdienste wie DHCP oder DNS in Ihrem Netzwerk zur Verfügung stellt, verwenden Sie die *Traditionelle Methode mit ifup*. Beim Einsatz von NetworkManager sollte `nm-applet` verwendet werden, um Netzwerkoptionen zu konfigurieren. Die Karteireiter *Übersicht*, *Hostname/DNS* und *Routing* des Moduls *Netzwerkeinstellungen* sind dann deaktiviert. Weitere Informationen zu NetworkManager finden Sie unter Kapitel 23, *Verwenden von NetworkManager* (S. 359).

Geben Sie unter *IPv6 Protocol Settings* (IPv6-Protokolleinstellungen) an, ob Sie das IPv6-Protokoll verwenden möchten. IPv6 kann parallel zu IPv4 verwendet werden. IPv6 ist standardmäßig aktiviert. In Netzwerken, die das IPv6-Protokoll nicht verwenden, können die Antwortzeiten jedoch schneller sein, wenn dieses Protokoll deaktiviert ist. Zum Deaktivieren von IPv6 deaktivieren Sie die Option *IPv6 aktivieren*. Dadurch wird das automatische Laden des Kernel-Moduls von IPv6 unterbunden. Die Einstellungen werden nach einem Neustart übernommen.

Unter *Optionen für DHCP-Client* konfigurieren Sie die Optionen für den DHCP-Client. Wenn der DHCP-Client den Server anweisen soll, seine Antworten immer per Broadcast zu versenden, aktivieren Sie *Broadcast-Antwort anfordern*. Diese Einstellung ist vermutlich erforderlich, wenn Sie Ihren Computer in verschiedenen Netzwerken verwenden. Die *Kennung für DHCP-Client* muss innerhalb eines Netzwerks für jeden DHCP-Client eindeutig sein. Wenn dieses Feld leer bleibt, wird standardmäßig die Hardware-Adresse der Netzwerkschnittstelle als Kennung übernommen. Falls Sie allerdings mehrere virtuelle Computer mit der gleichen Netzwerkschnittstelle und damit der gleichen Hardware-Adresse ausführen, sollten Sie hier eine eindeutige Kennung in beliebigem Format eingeben.

Unter *Zu sendender Hostname* wird eine Zeichenkette angegeben, die für das Optionsfeld "Hostname" verwendet wird, wenn dhcpcd Nachrichten an den DHCP-Server sendet. Einige DHCP-Server aktualisieren Namenserver-Zonen gemäß diesem Hostnamen (dynamischer DNS). Bei einigen DHCP-Servern muss das Optionsfeld *Zu sendender Hostname* in den DHCP-Nachrichten der Clients zudem eine bestimmte Zeichenkette enthalten. Übernehmen Sie die Einstellung `AUTO`, um den aktuellen Hostnamen zu senden (d. h. der aktuelle in `/etc/HOSTNAME` festgelegte Hostname). Lassen Sie das Optionsfeld leer, wenn kein Hostname gesendet werden soll. Wenn die Standardroute nicht gemäß der Informationen von DHCP geändert werden soll, deaktivieren Sie *Standardroute über DHCP ändern*.

Ändern der Konfiguration einer Netzwerkkarte

Wenn Sie die Konfiguration einer Netzwerkkarte ändern möchten, wählen Sie die Karte aus der Liste der erkannten Karten unter *Netzwerkeinstellungen > Übersicht* in YaST und klicken Sie auf *Bearbeiten*. Das Dialogfeld *Netzwerkkarten-Setup* wird angezeigt. Hier können Sie die Kartenkonfiguration auf den Karteireitern *Allgemein*, *Adresse* und *Hardware* anpassen. Genauere Informationen zur drahtlosen Kartenkonfiguration finden Sie unter Abschnitt 18.1.2, „Konfiguration mit YaST“ (S. 291).

IP-Adressen konfigurieren

Die IP-Adresse der Netzwerkkarte oder die Art der Festlegung dieser IP-Adresse kann auf dem Karteireiter *Adresse* im Dialogfeld *Einrichten der Netzwerkkarte* festgelegt werden. Die Adressen IPv4 und IPv6 werden unterstützt. Für die Netzwerkkarte können die Einstellungen *Keine IP-Adresse* (nützlich für eingebundene Geräte), *Statisch zugewiesene IP-Adresse* (IPv4 oder IPv6) oder *Dynamische Adresse* über *DHCP* und/oder *Zeroconf* zugewiesen werden.

Wenn Sie *Dynamische Adresse* verwenden, wählen Sie, ob *Nue DHCP-Version 4* (für IPv4), *Nur DHCP-Version 6* (für IPv6) oder *DHCP-Version 4 und 6* verwendet werden soll.

Wenn möglich wird die erste Netzwerkkarte mit einer Verbindung, die bei der Installation verfügbar ist, automatisch zur Verwendung der automatischen Adressenkonfiguration mit DHCP konfiguriert. Auf dem SUSE Linux Enterprise Desktop, auf dem NetworkManager standardmäßig aktiv ist, werden alle Netzwerkkarten konfiguriert.

ANMERKUNG: IBM-System z und DHCP

Auf IBM-System z-Plattformen wird die DHCP-basierte Adressenkonfiguration nur mit Netzwerkkarten unterstützt, die über eine MAC-Adresse verfügen. Das ist nur der Fall bei OSA- und OSA Express-Karten.

DHCP sollten Sie auch verwenden, wenn Sie eine DSL-Leitung verwenden, Ihr ISP (Internet Service Provider) Ihnen aber keine statische IP-Adresse zugewiesen hat. Wenn Sie DHCP verwenden möchten, konfigurieren Sie dessen Einstellungen im Dialogfeld *Netzwerkeinstellungen* des YaST-Konfigurationsmodul für Netzwerkkarten auf dem Karteireiter *Globale Optionen* unter *Optionen für DHCP-Client*. Geben Sie unter *Broadcast-Antwort anfordern* an, ob der DHCP-Client den Server anweisen soll, seine Antworten immer per Broadcast zu versenden. Diese Einstellung ist vermutlich erforderlich, wenn Sie Ihren Computer als mobilen Client in verschiedenen Netzwerken verwenden. In einer virtuellen Hostumgebung, in der mehrere Hosts über dieselbe Schnittstelle kommunizieren, müssen diese anhand der *Kennung für DHCP-Client* unterschieden werden.

DHCP eignet sich gut zur Client-Konfiguration, aber zur Server-Konfiguration ist es nicht ideal. Wenn Sie eine statische IP-Adresse festlegen möchten, gehen Sie wie folgt vor:

1. Wählen Sie im YaST-Konfigurationsmodul für Netzwerkkarten auf dem Karteireiter *Übersicht* aus der Liste der erkannten Karten eine Netzwerkkarte aus und klicken Sie auf *Bearbeiten*.

2. Wählen Sie auf dem Karteireiter *Adresse* die Option *Statisch zugewiesene IP-Adresse* aus.

3. Geben Sie die *IP-Adresse* ein. Es können beide Adressen, IPv4 und IPv6, verwendet werden. Geben Sie die Netzwerkmaske in *Teilnetzmaske* ein. Wenn die IPv6-Adresse verwendet wird, benutzen Sie *Teilnetzmaske* für die Präfixlänge im Format `/64`.

   Optional kann ein voll qualifizierter *Hostname* für diese Adresse eingegeben werden, der in die Konfigurationsdatei `/etc/hosts` geschrieben wird.

4. Klicken Sie auf *Weiter*.

5. Klicken Sie auf *OK*, um die Konfiguration zu aktivieren.

Wenn Sie die statische Adresse verwenden, werden die Namenserver und das Standard-Gateway nicht automatisch konfiguriert. Informationen zur Konfiguration von Namenservern finden Sie unter „Konfigurieren des Hostnamens und DNS“ (S. 250). Informationen zur Konfiguration eines Gateways finden Sie unter „Konfigurieren des Routing“ (S. 252).

Konfigurieren von Aliassen

Ein Netzwerkgerät kann mehrere IP-Adressen haben, die Aliasse genannt werden. Wenn Sie einen Alias für Ihre Netzwerkkarte einrichten möchten, gehen Sie wie folgt vor.

1. Wählen Sie im YaST-Konfigurationsmodul für Netzwerkkarten auf dem Karteireiter *Übersicht* aus der Liste der erkannten Karten eine Netzwerkkarte aus und klicken Sie auf *Bearbeiten*.

2. Klicken Sie auf dem Karteireiter *Adresse* > *Zusätzliche Adressen* auf *Hinzufügen*.

3. Geben Sie den *Aliasnamen*, die *IP-Adresse* und die *Netzmaske* ein. Nehmen Sie den Schnittstellennamen nicht in den Aliasnamen auf.

4. Klicken Sie auf *OK*.

5. Klicken Sie auf *Weiter*.

6. Klicken Sie auf *OK*, um die Konfiguration zu aktivieren.

Ändern des Gerätenamens und der Udev-Regeln

Der Gerätename der Netzwerkkarte kann während des laufenden Betriebs geändert werden. Es kann auch festgelegt werden, ob udev die Netzwerkkarte über die Hardware-Adresse (MAC) oder die Bus-ID erkennen soll. Die zweite Option ist bei großen Servern vorzuziehen, um einen Austausch der Karten unter Spannung zu erleichtern. Mit YaST legen Sie diese Optionen wie folgt fest:

1. Wählen Sie im YaST-Modul *Netzwerkeinstellungen* auf dem Karteireiter *Übersicht* aus der Liste der erkannten Karten eine Netzwerkkarte aus und klicken Sie auf *Bearbeiten*.

2. Öffnen Sie den Karteireiter *Hardware*. Der aktuelle Gerätename wird unter *Udev-Regeln* angezeigt. Klicken Sie auf *Ändern*.

3 Wählen Sie aus, ob udev die Karte über die *MAC-Adresse* oder die *Bus-ID* erkennen soll. Die aktuelle MAC-Adresse und Bus-ID der Karte werden im Dialogfeld angezeigt.

4 Aktivieren Sie zum Ändern des Gerätenamens die Option *Gerätenamen ändern* und bearbeiten Sie den Namen.

5 Klicken Sie auf *OK* und *Weiter*.

6 Klicken Sie auf *OK*, um die Konfiguration zu aktivieren.

Ändern des Kernel-Treibers für Netzwerkkarten

Für einige Netzwerkkarten sind eventuell verschiedene Kernel-Treiber verfügbar. Wenn die Karte bereits konfiguriert ist, ermöglicht YaST die Auswahl eines zu verwendenden Kernel-Treibers aus einer Liste verfügbarer Treiber. Es ist auch möglich, Optionen für den Kernel-Treiber anzugeben. Mit YaST legen Sie diese Optionen wie folgt fest:

1 Wählen Sie im YaST-Modul Netzwerkeinstellungen auf dem Karteireiter *Übersicht* aus der Liste der erkannten Karten eine Netzwerkkarte aus und klicken Sie auf *Bearbeiten*.

2 Öffnen Sie den Karteireiter *Hardware*.

3 Wählen Sie den zu verwendenden Kernel-Treiber unter *Modulname* aus. Geben Sie die entsprechenden Optionen für den ausgewählten Treiber unter *Optionen* im Format `Option=Wert` ein. Wenn mehrere Optionen verwendet werden, sollten sie durch Leerzeichen getrennt sein.

4 Klicken Sie auf *OK* und *Weiter*.

5 Klicken Sie auf *OK*, um die Konfiguration zu aktivieren.

Aktivieren des Netzwerkgeräts

Wenn Sie die traditionelle Methode mit ifup verwenden, können Sie Ihr Gerät so konfigurieren, dass es wahlweise beim Systemstart, bei der Verbindung per Kabel, beim Erkennen der Karte, manuell oder nie startet. Wenn Sie den Gerätestart ändern möchten, gehen Sie wie folgt vor:

1. Wählen Sie in YaST eine Karte aus der Liste der erkannten Karten unter *Netzwerkgeräte* > *Netzwerkeinstellungen* und klicken Sie auf *Bearbeiten*.

2. In der Karteireiter *Allgemein* wählen Sie den gewünschten Eintrag unter *Geräte-Aktivierung*.

   Wählen Sie *Beim Systemstart*, um das Gerät beim Booten des Systems zu starten. Wenn *Bei Kabelanschluss* aktiviert ist, wird die Schnittstelle auf physikalische Netzwerkverbindungen überwacht. Wenn *Falls hot-plugged* aktiviert ist, wird die Schnittstelle eingerichtet, sobald sie verfügbar ist. Dies gleicht der Option *Bei Systemstart*, führt jedoch nicht zu einem Fehler beim Systemstart, wenn die Schnittstelle nicht vorhanden ist. Wählen Sie *Manuell*, wenn die Schnittstelle manuell mit `ifup` oder KInternet gesteuert werden soll. Wählen Sie *Nie*, wenn das Gerät gar nicht gestartet werden soll. *Bei NFSroot* verhält sich ähnlich wie *Beim Systemstart*, allerdings fährt das Kommando `rcnetwork stop` die Schnittstelle bei dieser Einstellung nicht herunter. Diese Einstellung empfiehlt sich bei einem NFS- oder iSCSI-Root-Dateisystem.

3. Klicken Sie auf *Weiter*.

4. Klicken Sie auf *OK*, um die Konfiguration zu aktivieren.

Normalerweise können Netzwerk-Schnittstellen nur vom Systemadministrator aktiviert und deaktiviert werden. Wenn Benutzer in der Lage sein sollen, diese Schnittstelle über KInternet zu aktivieren, wählen Sie *Gerätesteuerung für Nicht-Root-Benutzer über KInternet aktivieren* aus.

Einrichten der Größe der maximalen Transfereinheit

Sie können eine maximale Transfereinheit (MTU) für die Schnittstelle festlegen. MTU bezieht sich auf die größte zulässige Paketgröße in Byte. Eine größere MTU bringt eine höhere Bandbreiteneffizienz. Große Pakete können jedoch eine langsame Schnittstelle für einige Zeit belegen und die Verzögerung für nachfolgende Pakete vergrößern.

1. Wählen Sie in YaST eine Karte aus der Liste der erkannten Karten unter *Netzwerkgeräte* > *Netzwerkeinstellungen* und klicken Sie auf *Bearbeiten*.

2. Wählen Sie im Karteireiter *Allgemein* den gewünschten Eintrag aus der Liste *Set MTU* (MTU festlegen).

3 Klicken Sie auf *Weiter*.

4 Klicken Sie auf *OK*, um die Konfiguration zu aktivieren.

Konfigurieren der Firewall

Sie müssen nicht die genaue Firewall-Konfiguration durchführen, wie unter Abschnitt „Configuring the Firewall with YaST“ (Kapitel 8, *Masquerading and Firewalls*, ↑*Security Guide*) beschrieben. Sie können einige grundlegende Firewall-Einstellungen für Ihr Gerät als Teil der Gerätekonfiguration festlegen. Führen Sie dazu die folgenden Schritte aus:

1 Öffnen Sie das YaST-Modul *Netzwerkgeräte* > *Netzwerkeinstellungen*. Wählen Sie im Karteireiter *Übersicht* eine Karte aus der Liste erkannter Karten und klicken Sie auf *Bearbeiten*.

2 Öffnen Sie den Karteireiter *Allgemein* des Dialogfelds *Netzwerkeinstellungen*.

3 Legen Sie die Firewall-Zone fest, der Ihre Schnittstelle zugewiesen werden soll. Mit den zur Verfügung stehenden Optionen können Sie

Firewall deaktiviert
: Diese Option ist nur verfügbar, wenn die Firewall deaktiviert ist und die Firewall überhaupt nicht ausgeführt wird. Verwenden Sie diese Option nur, wenn Ihr Computer Teil eines größeren Netzwerks ist, das von einer äußeren Firewall geschützt wird.

Automatisches Zuweisen von Zonen
: Diese Option ist nur verfügbar, wenn die Firewall aktiviert ist. Die Firewall wird ausgeführt und die Schnittstelle wird automatisch einer Firewall-Zone zugewiesen. Die Zone, die das Stichwort `Beliebig` enthält, oder die externe Zone wird für solch eine Schnittstelle verwendet.

Interne Zone (ungeschützt)
: Die Firewall wird ausgeführt, aber es gibt keine Regeln, die diese Schnittstelle schützen. Verwenden Sie diese Option, wenn Ihr Computer Teil eines größeren Netzwerks ist, das von einer äußeren Firewall geschützt wird. Sie ist auch nützlich für die Schnittstellen, die mit dem internen Netzwerk verbunden sind,wenn der Computer über mehrere Netzwerkschnittstellen verfügt.

Demilitarisierte Zone
: Eine demilitarisierte Zone ist eine zusätzliche Verteidigungslinie zwischen einem internen Netzwerk und dem (feindlichen) Internet. Die dieser Zone zugewiesenen Hosts können vom internen Netzwerk und vom Internet erreicht werden, können jedoch nicht auf das interne Netzwerk zugreifen.

Externe Zone
: Die Firewall wird an dieser Schnittstelle ausgeführt und schützt sie vollständig vor anderem (möglicherweise feindlichem) Netzwerkverkehr. Dies ist die Standardoption.

4. Klicken Sie auf *Weiter*.

5. Aktivieren Sie die Konfiguration, indem Sie auf *OK* klicken.

Konfigurieren einer unerkannten Netzwerkkarte

Ihre Karte wird unter Umständen nicht richtig erkannt. In diesem Fall erscheint sie nicht in der Liste der erkannten Karten. Wenn Sie sich nicht sicher sind, ob Ihr System über einen Treiber für die Karte verfügt, können Sie sie manuell konfigurieren. Sie können auch spezielle Netzwerkgerätetypen konfigurieren, z. B. Bridge, Bond, TUN oder TAP. So konfigurieren Sie eine nicht erkannte Netzwerkkarte oder ein spezielles Gerät:

1. Klicken Sie im Dialogfeld *Netzwerkgeräte* > *Netzwerkeinstellungen* > *Übersicht* in YaST auf *Hinzufügen*.

2. Legen Sie den *Gerätetyp* der Schnittstelle im Dialogfeld *Hardware* mit Hilfe der verfügbaren Optionen fest und geben Sie einen *Konfigurationsnamen* ein. Wenn es sich bei der Netzwerkkarte um ein PCMCIA- oder USB-Gerät handelt, aktivieren Sie das entsprechende Kontrollkästchen und schließen Sie das Dialogfeld durch Klicken auf *Weiter*. Ansonsten können Sie den Kernel *Modulname* definieren, der für die Karte verwendet wird, sowie gegebenenfalls dessen *Optionen*.

3. Klicken Sie auf *Weiter*.

4. Konfigurieren Sie die benötigten Optionen wie die IP-Adresse, die Geräteaktivierung oder die Firewall-Zone für die Schnittstelle auf den Karteireitern *Allgemein*, *Adresse* und *Hardware*. Weitere Informationen zu den Konfigurationsoptionen finden Sie in „Ändern der Konfiguration einer Netzwerkkarte“ (S. 243).

5 Wenn Sie für den Gerätetyp der Schnittstelle die Option *Drahtlos* gewählt haben, konfigurieren Sie im nächsten Dialogfeld die drahtlose Verbindung. Weitere Informationen zur Konfiguration drahtloser Geräte erhalten Sie unter Abschnitt 18.1, „Wireless LAN“ (S. 287).

6 Klicken Sie auf *Weiter*.

7 Klicken Sie auf *OK*, um die neue Netzwerkkonfiguration zu aktivieren.

Konfigurieren des Hostnamens und DNS

Wenn Sie die Netzwerkkonfiguration während der Installation noch nicht geändert haben und die verkabelte Karte bereits verfügbar war, wurde automatisch ein Hostname für Ihren Computer erstellt und DHCP wurde aktiviert. Dasselbe gilt für die Namensservicedaten, die Ihr Host für die Integration in eine Netzwerkumgebung benötigt. Wenn DHCP für eine Konfiguration der Netzwerkadresse verwendet wird, wird die Liste der Domain Name Server automatisch mit den entsprechenden Daten versorgt. Falls eine statische Konfiguration vorgezogen wird, legen Sie diese Werte manuell fest.

Wenn Sie den Namen Ihres Computers und die Namenserver-Suchliste ändern möchten, gehen Sie wie folgt vor:

1 Wechseln Sie zum Karteireiter *Netzwerkeinstellungen* > *Hostname/DNS* im Modul *Netzwerkgeräte* in YaST.

2 Geben Sie den *Hostnamen* und bei Bedarf auch den *Domänennamen* ein. Die Domäne ist besonders wichtig, wenn der Computer als Mailserver fungiert. Der Hostname ist global und gilt für alle eingerichteten Netzwerkschnittstellen.

   Wenn Sie zum Abrufen einer IP-Adresse DHCP verwenden, wird der Hostname Ihres Computers automatisch durch DHCP festgelegt. Sie sollten dieses Verhalten deaktivieren, wenn Sie Verbindungen zu verschiedenen Netzwerken aufbauen, da Sie verschiedene Hostnamen zuweisen können und das Ändern des Hostnamens beim Ausführen den grafischen Desktop verwirren kann. Zum Deaktivieren von DHCP, damit Sie eine IP-Adresse erhalten, deaktivieren Sie *Hostnamen über DHCP ändern*.

   Wenn Sie DHCP zum Abrufen einer IP-Adresse verwenden, wird Ihr Hostname standardmäßig in die Datei `/etc/hosts` geschrieben. Der Name kann in diesem Fall als `127.0.0.2`-IP-Adresse aufgelöst werden. Um dieses Standardverhalten

zu unterbinden, deaktivieren Sie *Hostname in /etc/hosts schreiben*. Allerdings kann Ihr Hostname dann ohne aktives Netzwerk nicht aufgelöst werden.

3 Legen Sie unter *DNS-Konfiguration ändern* fest, wie die DNS-Konfiguration (Namenserver, Suchliste, Inhalt der Datei `/etc/resolv.conf`) geändert wird.

Wenn die Option *Standardrichtlinie verwenden* ausgewählt ist, wid die Konfiguration vom Skript `netconfig` verwaltet, das die statisch definierten Daten (mit YaST oder in den Konfigurationsdateien) mit dynamisch bezogenen Daten (vom DHCP-Client oder NetworkManager) zusammenführt. Diese Standardrichtlinie ist in den meisten Fällen ausreichend.

Wenn die Option *Nur manuell* ausgewählt ist, darf `netconfig` die Datei `/etc/resolv.conf` nicht ändern. Jedoch kann diese Datei manuell bearbeitet werden.

Wenn die Option *Custom Policy* (Benutzerdefinierte Richtlinie) ausgewählt ist, muss eine Zeichenkette für die *benutzerdefinierte Richtlinienrege* angegeben werden, welche die Zusammenführungsrichtlinie definiert. Die Zeichenkette besteht aus einer durch Kommas getrennte Liste mit Schnittstellennamen, die als gültige Quelle für Einstellungen betrachtet werden. Mit Ausnahme von vollständigen Schnittstellennamen sind auch grundlegende Platzhalterzeichen für die Entsprechung mit mehreren Schnittstellen zulässig. Beispiel: `eth* ppp?` richtet sich zuerst an alle eth- und dann an alle ppp0-ppp9-Schnittstellen. Es gibt zwei spezielle Richtlinienwerte, die angeben, wie die statischen Einstellungen angewendet werden, die in der Datei `/etc/sysconfig/network/config` definiert sind:

`STATIC`
: Die statischen Einstellungen müssen mit den dynamischen Einstellungen zusammengeführt werden.

`STATIC_FALLBACK`
: Die statischen Einstellungen werden nur verwendet, wenn keine dynamische Konfiguration verfügbar ist.

Weitere Informationen finden Sie unter `man 8 netconfig`.

4 Geben Sie die *Namenserver* ein und füllen Sie die *Domänensuchliste* aus. Nameserver müssen in der IP-Adresse angegeben werden, wie zum Beispiel

192.168.1.116, nicht im Hostnamen. Namen, die im Karteireiter *Domänensuche* angegeben werden, sind Namen zum Auflösen von Hostnamen ohne angegebene Domäne. Wenn mehr als eine *Suchdomäne* verwendet wird, müssen die Domänen durch Kommas oder Leerzeichen getrennt werden.

5 Klicken Sie auf *OK*, um die Konfiguration zu aktivieren.

Konfigurieren des Routing

Damit Ihre Maschine mit anderen Maschinen und Netzwerken kommuniziert, müssen Routing-Daten festgelegt werden. Dann nimmt der Netzwerkverkehr den korrekten Weg. Wird DHCP verwendet, werden diese Daten automatisch angegeben. Wird eine statische Konfiguration verwendet, müssen Sie die Daten manuell angeben.

1 Navigieren Sie in YaST zu *Netzwerkeinstellungen* > *Routing*.

2 Geben Sie die IP-Adresse des *Standard-Gateway* ein. Der Standard-Gateway entspricht jedem möglichen Ziel, wenn aber ein anderer Eintrag der erforderlichen Adresse entspricht, wird diese anstelle der Standardroute verwendet.

3 In der *Routing-Tabelle* können weitere Einträge vorgenommen werden. Geben Sie die IP-Adresse für das *Ziel*-Netzwerk, die IP-Adresse des *Gateways* und die *Netzmaske* ein. Wählen Sie das *Gerät* aus, durch das der Datenverkehr zum definierten Netzwerk geroutet wird (das Minuszeichen steht für ein beliebiges Gerät). Verwenden Sie das Minuszeichen –, um diese Werte frei zu lassen. Verwenden Sie `Standard` im Feld *Ziel*, um in der Tabelle ein Standard-Gateway einzugeben.

ANMERKUNG

Wenn mehrere Standardrouten verwendet werden, kann die Metrik-Option verwendet werden, um festzulegen, welche Route eine höhere Priorität hat. Geben Sie zur Angabe der Metrik-Option `– Metrik` *`Nummer`* unter *Optionen* ein. Die Route mit der höchsten Metrik wird als Standard verwendet. Wenn das Netzwerkgerät getrennt wird, wird seine Route entfernt und die nächste verwendet. Der aktuelle Kernel verwendet jedoch keine Metrik bei statischem Routing, sondern nur ein Routing-Daemon wie multipathd.

4 Wenn das System ein Router ist, aktivieren Sie die Option *IP-Weiterleitung* in den *Netzwerkeinstellungen*.

5 Klicken Sie auf *OK*, um die Konfiguration zu aktivieren.

17.4.2 Modem

TIPP: IBM-System z: Modem

Die Konfiguration dieses Hardwaretyps wird auf den IBM-System z-Plattformen nicht unterstützt.

Im YaST-Kontrollzentrum greifen Sie mit *Netzwerkgeräte* > *Modem* auf die Modem-Konfiguration zu. Wenn Ihr Modem nicht automatisch erkannt wurde, wechseln Sie zum Karteireiter *Modemgeräte* und öffnen Sie das Dialogfeld für manuelle Konfiguration, indem Sie auf *Hinzufügen* klicken. Geben Sie unter *Modemgerät* die Schnittstelle an, an die das Modem angeschlossen ist.

TIPP: CDMA- und GPRS-Modems

Konfigurieren Sie unterstützte CDMA- und GPRS-Modems mit dem YaST-*Modem*-Modul wie reguläre Modems.

Abbildung 17.4 *Modemkonfiguration*

Wenn eine Telefonanlage zwischengeschaltet ist, müssen Sie ggf. eine Vorwahl für die Amtsholung eingeben. Dies ist in der Regel die Null. Sie können diese aber auch in der Bedienungsanleitung der Telefonanlage finden. Zudem können Sie festlegen, ob Ton- oder Impulswahl verwendet, der Lautsprecher eingeschaltet und der Wählton abgewartet werden soll. Letztere Option sollte nicht verwendet werden, wenn Ihr Modem an einer Telefonanlage angeschlossen ist.

Legen Sie unter *Details* die Baudrate und die Zeichenketten zur Modeminitialisierung fest. Ändern Sie die vorhandenen Einstellungen nur, wenn das Modem nicht automatisch erkannt wird oder es spezielle Einstellungen für die Datenübertragung benötigt. Dies ist vor allem bei ISDN-Terminaladaptern der Fall. Schließen Sie das Dialogfeld mit *OK*. Wenn Sie die Kontrolle des Modems an normale Benutzer ohne Root-Berechtigung abgeben möchten, aktivieren Sie *Enable Device Control for Non-root User via KInternet* (Gerätesteuerung für Nicht-Root-Benutzer via KInternet ermöglichen). Auf diese Weise kann ein Benutzer ohne Administratorberechtigungen eine Schnittstelle aktivieren oder deaktivieren. Geben Sie unter *Regulärer Ausdruck für Vorwahl zur Amtsholung* einen regulären Ausdruck an. Dieser muss der vom Benutzer unter *Dial Prefix* (Vorwahl) in KInternet bearbeitbaren Vorwahl entsprechen. Wenn dieses Feld leer ist, kann ein Benutzer ohne Administratorberechtigungen keine andere *Vorwahl* festlegen.

Wählen Sie im nächsten Dialogfeld den ISP (Internet Service Provider). Wenn Sie Ihren Provider aus einer Liste der für Ihr Land verfügbaren Provider auswählen möchten, aktivieren Sie *Land*. Sie können auch auf *Neu* klicken, um ein Dialogfeld zu öffnen, in dem Sie die Daten Ihres ISPs eingeben können. Dazu gehören ein Name für die Einwahlverbindung und den ISP sowie die vom ISP zur Verfügung gestellten Benutzer- und Kennwortdaten für die Anmeldung. Aktivieren Sie *Immer Passwort abfragen*, damit immer eine Passwortabfrage erfolgt, wenn Sie eine Verbindung herstellen.

Im letzten Dialogfeld können Sie zusätzliche Verbindungsoptionen angeben:

Dial-On-Demand
: Wenn Sie *Dial-on-Demand* aktivieren, müssen Sie mindestens einen Namenserver angeben. Verwenden Sie diese Funktion nur, wenn Sie über eine günstige Internet-Verbindung oder eine Flatrate verfügen, da manche Programme in regelmäßigen Abständen Daten aus dem Internet abfragen.

Während Verbindung DNS ändern
: Diese Option ist standardmäßig aktiviert, d. h. die Adresse des Namenservers wird bei jeder Verbindung mit dem Internet automatisch aktualisiert.

DNS automatisch abrufen
: Wenn der Provider nach dem Herstellen der Verbindung seinen DNS-Server nicht überträgt, deaktivieren Sie diese Option und geben Sie die DNS-Daten manuell ein.

Automatically Reconnect (Automatische Verbindungswiederherstellung)
: Wenn aktiviert, wird nach einem Fehler automatisch versucht, die Verbindung wiederherzustellen.

Ignoriere Eingabeaufforderung
: Diese Option deaktiviert die Erkennung der Eingabeaufforderungen des Einwahlservers. Aktivieren Sie diese Option, wenn der Verbindungsaufbau sehr lange dauert oder die Verbindung nicht zustande kommt.

Externe Firewall-Schnittstelle
: Durch Auswahl dieser Option wird die Firewall aktiviert und die Schnittstelle als extern festgelegt. So sind Sie für die Dauer Ihrer Internetverbindung vor Angriffen von außen geschützt.

Idle-Time-Out (Sekunden)
: Mit dieser Option legen Sie fest, nach welchem Zeitraum der Netzwerkinaktivität die Modemverbindung automatisch getrennt wird.

IP-Details
: Diese Option öffnet das Dialogfeld für die Adresskonfiguration. Wenn Ihr ISP Ihrem Host keine dynamische IP-Adresse zuweist, deaktivieren Sie die Option *Dynamische IP-Adresse* und geben Sie die lokale IP-Adresse des Hosts und anschließend die entfernte IP-Adresse ein. Diese Informationen erhalten Sie von Ihrem ISP. Lassen Sie die Option *Standard-Route* aktiviert und schließen Sie das Dialogfeld mit *OK*.

Durch Auswahl von *Weiter* gelangen Sie zum ursprünglichen Dialogfeld zurück, in dem eine Zusammenfassung der Modemkonfiguration angezeigt wird. Schließen Sie das Dialogfeld mit *OK*.

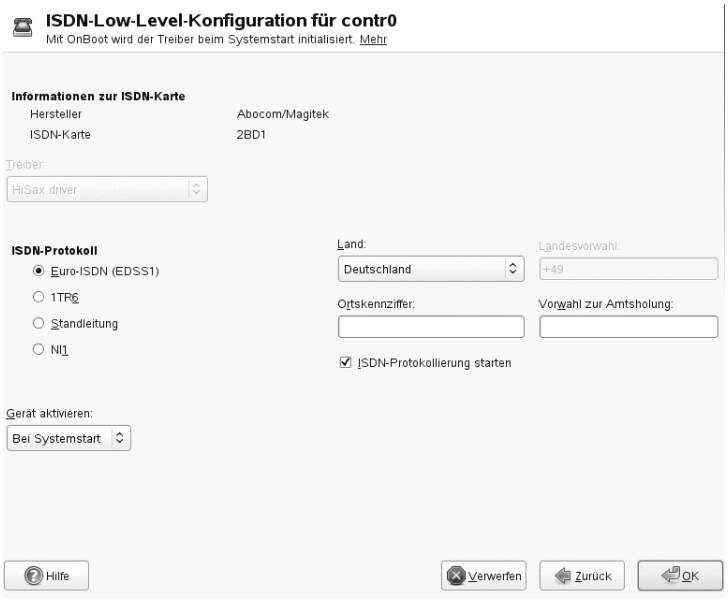
17.4.3 ISDN

TIPP: IBM-System z: ISDN

Die Konfiguration dieses Hardwaretyps wird auf den IBM-System z-Plattformen nicht unterstützt.

Dieses Modul ermöglicht die Konfiguration einer oder mehrerer ISDN-Karten in Ihrem System. Wenn YaST Ihre ISDN-Karte nicht erkannt hat, klicken Sie auf dem Karteireiter *ISDN-Geräte* auf *Hinzufügen* und wählen Sie Ihre Karte manuell aus. Theoretisch können Sie mehrere Schnittstellen einrichten, im Normalfall ist dies aber nicht notwendig, da Sie für eine Schnittstelle mehrere Provider einrichten können. Die nachfolgenden Dialogfelder dienen dann dem Festlegen der verschiedenen ISDN-Optionen für den ordnungsgemäßen Betrieb der Karte.

Abbildung 17.5 *ISDN-Konfiguration*



Wählen Sie im nächsten Dialogfeld, das in Abbildung 17.5, „ISDN-Konfiguration“ (S. 257) dargestellt ist, das zu verwendende Protokoll. Der Standard ist *Euro-ISDN (EDSS1)*, aber für ältere oder größere Telefonanlagen wählen Sie *1TR6*. Für die USA gilt *NI1*. Wählen Sie das Land in dem dafür vorgesehenen Feld aus. Die entsprechende Landeskennung wird im Feld daneben angezeigt. Geben Sie dann noch die *Ortsnetzkennzahl* und ggf. die *Vorwahl zur Amtsholung* ein. Wenn nicht der gesamte ISDN-Datenverkehr protokolliert werden soll, deaktivieren Sie die Option *ISDN-Protokollierung starten*.

Geräte-Aktivierung definiert, wie die ISDN-Schnittstelle gestartet werden soll: *Beim Systemstart* initialisiert den ISDN-Treiber bei jedem Systemstart. Bei *Manuell* müssen Sie den ISDN-Treiber als `root` laden. Verwenden Sie hierfür den Befehl `rcisdn start`. *Falls hot-plugged* wird für PCMCIA- oder USB-Geräte verwendet. Diese Option lädt den Treiber, nachdem das Gerät eingesteckt wurde. Wenn Sie alle Einstellungen vorgenommen haben, klicken Sie auf *OK*.

Im nächsten Dialogfeld können Sie den Schnittstellentyp für die ISDN-Karte angeben und weitere ISPs zu einer vorhandenen Schnittstelle hinzufügen. Schnittstellen können

in den Betriebsarten `SyncPPP` oder `RawIP` angelegt werden. Die meisten ISPs verwenden jedoch den `SyncPPP`-Modus, der im Folgenden beschrieben wird.

Abbildung 17.6 *Konfiguration der ISDN-Schnittstelle*

Die Nummer, die Sie unter *Eigene Telefonnummer* eingeben, ist vom jeweiligen Anschlussszenario abhängig:

ISDN-Karte direkt an der Telefondose
: Eine standardmäßige ISDN-Leitung bietet Ihnen drei Rufnummern (sogenannte MSNs, Multiple Subscriber Numbers). Auf Wunsch können (auch) bis zu zehn Rufnummern zur Verfügung gestellt werden. Eine dieser MSNs muss hier eingegeben werden, allerdings ohne Ortsnetzkennzahl. Sollten Sie eine falsche Nummer eintragen, wird Ihr Netzbetreiber die erste Ihrem ISDN-Anschluss zugeordnete MSN verwenden.

ISDN-Karte an einer Telefonanlage
: Auch hier kann die Konfiguration je nach installierten Komponenten variieren:

1. Kleinere Telefonanlagen für den Hausgebrauch verwenden für interne Anrufe in der Regel das Euro-ISDN-Protokoll (EDSS1). Diese Telefonanlagen haben einen internen S0-Bus und verwenden für die angeschlossenen Geräte interne Rufnummern.

   Für die Angabe der MSN verwenden Sie eine der internen Rufnummern. Eine der möglichen MSNs Ihrer Telefonanlage sollte funktionieren, sofern für diese der Zugriff nach außen freigeschaltet ist. Im Notfall funktioniert eventuell auch

eine einzelne Null. Weitere Informationen dazu entnehmen Sie bitte der Dokumentation Ihrer Telefonanlage.

2. Größere Telefonanlagen (z. B. in Unternehmen) verwenden für die internen Anschlüsse das Protokoll 1TR6. Die MSN heißt hier EAZ und ist üblicherweise die Durchwahl. Für die Konfiguration unter Linux ist die Eingabe der letzten drei Stellen der EAZ in der Regel ausreichend. Im Notfall probieren Sie die Ziffern 1 bis 9.

Wenn die Verbindung vor der nächsten zu zahlenden Gebühreneinheit getrennt werden soll, aktivieren Sie *ChargeHUP*. Dies funktioniert unter Umständen jedoch nicht mit jedem ISP. Durch Auswahl der entsprechenden Option können Sie auch die Kanalbündelung (Multilink-PPP) aktivieren. Sie können die Firewall für die Verbindung aktivieren, indem Sie *Externe Firewall-Schnittstelle* und *Firewall neu starten* auswählen. Wenn Sie normalen Benutzern ohne Administratorberechtigung die Aktivierung und Deaktivierung der Schnittstelle erlauben möchten, aktivieren Sie *Enable Device Control for Non-root user via KInternet* (Gerätesteuerung für Nicht-Root-Benutzer via KInternet ermöglichen).

Details öffnet ein Dialogfeld, das für die Implementierung komplexerer Verbindungsszenarien ausgelegt und aus diesem Grund für normale Heimbenutzer nicht relevant ist. Schließen Sie das Dialogfeld *Details* mit *OK*.

Im nächsten Dialogfeld legen Sie die Einstellungen für die Vergabe der IP-Adressen fest. Wenn Ihr Provider Ihnen keine statische IP-Adresse zugewiesen hat, wählen Sie *Dynamische IP-Adresse*. Anderenfalls tragen Sie gemäß den Angaben Ihres Providers die lokale IP-Adresse Ihres Rechners sowie die entfernte IP-Adresse in die dafür vorgesehenen Felder ein. Soll die anzulegende Schnittstelle als Standard-Route ins Internet dienen, aktivieren Sie *Standard-Route*. Beachten Sie, dass jeweils nur eine Schnittstelle pro System als Standard-Route in Frage kommt. Schließen Sie das Dialogfeld mit *Weiter*.

Im folgenden Dialogfeld können Sie Ihr Land angeben und einen ISP wählen. Bei den in der Liste aufgeführten ISPs handelt es sich um Call-By-Call-Provider. Wenn Ihr ISP in der Liste nicht aufgeführt ist, wählen Sie *Neu*. Dadurch wird das Dialogfeld *Provider-Parameter* geöffnet, in dem Sie alle Details zu Ihrem ISP eingeben können. Die Telefonnummer darf keine Leerzeichen oder Kommas enthalten. Geben Sie dann den Benutzernamen und das Passwort ein, den bzw. das Sie von Ihrem ISP erhalten haben. Wählen Sie anschließend *Weiter*.

Um auf einem Einzelplatz-Arbeitsplatzrechner *Dial-On-Demand* verwenden zu können, müssen Sie auf jeden Fall den Namenserver (DNS-Server) angeben. Die meisten Provider unterstützen heute die dynamische DNS-Vergabe, d. h. beim Verbindungsaufbau wird die IP-Adresse eines Namenservers übergeben. Bei einem Einzelplatz-Arbeitsplatzrechner müssen Sie dennoch eine Platzhalteradresse wie `192.168.22.99` angeben. Wenn Ihr ISP keine dynamischen DNS-Namen unterstützt, tragen Sie die IP-Adressen der Namenserver des ISPs ein. Ferner können Sie festlegen, nach wie vielen Sekunden die Verbindung automatisch getrennt werden soll, falls in der Zwischenzeit kein Datenaustausch stattgefunden hat. Bestätigen Sie die Einstellungen mit *Weiter*. YaST zeigt eine Zusammenfassung der konfigurierten Schnittstellen an. Klicken Sie zur Aktivierung dieser Einstellungen auf *OK*.

17.4.4 Kabelmodem

TIPP: IBM-System z: Kabelmodem

Die Konfiguration dieses Hardwaretyps wird auf den IBM-System z-Plattformen nicht unterstützt.

In einigen Ländern wird der Zugriff auf das Internet über Kabel-TV mehr und mehr üblich. Der TV-Kabel-Abonnent erhält in der Regel ein Modem, das auf der einen Seite an die TV-Kabelbuchse und auf der anderen Seite (mit einem 10Base-TG Twisted-Pair-Kabel) an die Netzwerkkarte des Computers angeschlossen wird. Das Kabelmodem stellt dann eine dedizierte Internetverbindung mit einer statischen IP-Adresse zur Verfügung.

Richten Sie sich bei der Konfiguration der Netzwerkkarte nach den Anleitungen Ihres ISP (Internet Service Provider) und wählen Sie entweder *Dynamic Address* (Dynamische Adresse) oder *Statically assigned IP address* (Statisch zugewiesene IP-Adresse) aus. Die meisten Provider verwenden heute DHCP. Eine statische IP-Adresse ist oft Teil eines speziellen Firmenkontos.

Weitere Informationen zur Konfiguration von Kabelmodems erhalten Sie im entsprechenden Artikel der Support-Datenbank. Dieser ist online verfügbar unter `http://en.opensuse.org/SDB:Setting_Up_an_Internet_Connection_via_Cable_Modem_with_SuSE_Linux_8.0_or_Higher`.

17.4.5 DSL

TIPP: IBM-System z: DSL

Die Konfiguration dieses Hardwaretyps wird auf den IBM-System z-Plattformen nicht unterstützt.

Um das DSL-Gerät zu konfigurieren, wählen Sie das *DSL*-Modul aus dem Abschnitt YaST*Netzwerkgeräte* aus. Dieses YaST-Modul besteht aus mehreren Dialogfeldern, in denen Sie die Parameter des DSL-Zugangs basierend auf den folgenden Protokollen festlegen können:

- PPP über Ethernet (PPPoE)
- PPP über ATM (PPPoATM)
- CAPI für ADSL (Fritz-Karten)
- Tunnel-Protokoll für Point-to-Point (PPTP) – Österreich

Im Dialogfeld *Überblick über die DSL-Konfiguration* finden Sie auf dem Karteireiter *DSL-Geräte* eine Liste der installierten DSL-Geräte. Zur Änderung der Konfiguration eines DSL-Geräts wählen Sie das Gerät in der Liste aus und klicken Sie auf *Bearbeiten*. Wenn Sie ein neues DSL-Gerät manuell konfigurieren möchten, klicken Sie auf *Hinzufügen*.

Beachten Sie bitte, dass die Konfiguration Ihres DSL-Zugangs mit PPPoE und PPTP eine korrekte Konfiguration der Netzwerkkarte voraussetzt. Falls noch nicht geschehen, konfigurieren Sie zunächst die Karte, indem Sie *Netzwerkkarten konfigurieren* auswählen (siehe Abschnitt 17.4.1, „Konfigurieren der Netzwerkkarte mit YaST“ (S. 240)). Bei DSL-Verbindungen können die Adressen zwar automatisch vergeben werden, jedoch nicht über DHCP. Aus diesem Grund dürfen Sie die Option *Dynamic Address* (Dynamische Adresse) nicht aktivieren. Geben Sie stattdessen eine statische Dummy-Adresse für die Schnittstelle ein, z. B. `192.168.22.1`. Geben Sie unter *Subnetzmaske* `255.255.255.0` ein. Wenn Sie eine Einzelplatz-Arbeitsstation konfigurieren, lassen Sie das Feld *Standard-Gateway* leer.

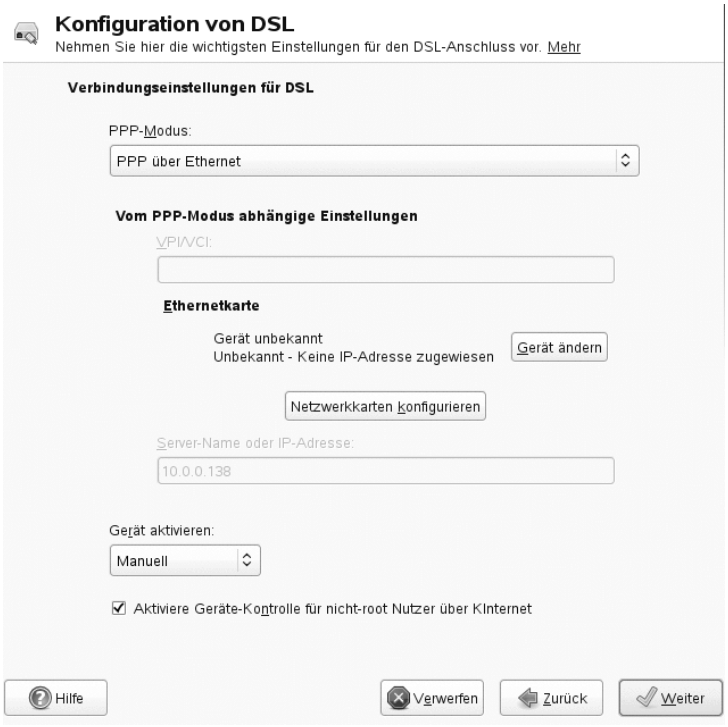
TIPP

Die Werte in den Feldern *IP-Adresse* und *Subnetzmaske* sind lediglich Platzhalter. Sie haben für den Verbindungsaufbau mit DSL keine Bedeutung und werden nur zur Initialisierung der Netzwerkkarte benötigt.

Wählen Sie im ersten Dialogfeld für die DSL-Konfiguration (siehe Abbildung 17.7, „DSL-Konfiguration“ (S. 263)) den *PPP-Modus* und die *Ethernetkarte*, mit der das DSL-Modem verbunden ist (in den meisten Fällen ist dies `eth0`). Geben Sie anschließend unter *Geräte-Aktivierung* an, ob die DSL-Verbindung schon beim Booten des Systems gestartet werden soll. Aktivieren Sie *Enable Device Control for Non-root User via KInternet* (Gerätesteuerung für Nicht-Root-Benutzer via KInternet ermöglichen), wenn Sie normalen Benutzern ohne Root-Berechtigung die Aktivierung und Deaktivierung der Schnittstelle via KInternet erlauben möchten.

Wählen Sie im nächsten Dialogfeld Ihr Land aus und treffen Sie eine Auswahl aus den ISPs, die in Ihrem Land verfügbar sind. Die Inhalte der danach folgenden Dialogfelder der DSL-Konfiguration hängen stark von den bis jetzt festgelegten Optionen ab und werden in den folgenden Abschnitten daher nur kurz angesprochen. Weitere Informationen zu den verfügbaren Optionen erhalten Sie in der ausführlichen Hilfe in den einzelnen Dialogfeldern.

Abbildung 17.7 *DSL-Konfiguration*



Um auf einem Einzelplatz-Arbeitsplatzrechner *Dial-On-Demand* verwenden zu können, müssen Sie auf jeden Fall den Namenserver (DNS-Server) angeben. Die meisten Provider unterstützen die dynamische DNS-Vergabe, d. h. beim Verbindungsaufbau wird die IP-Adresse eines Namenservers übergeben. Bei einem Einzelplatz-Arbeitsplatzrechner müssen Sie jedoch eine Platzhalteradresse wie `192.168.22.99` angeben. Wenn Ihr ISP keine dynamische DNS-Namen unterstützt, tragen Sie die IP-Adressen der Namenserver des ISPs ein.

Idle-Timeout (Sekunden) definiert, nach welchem Zeitraum der Netzwerkinaktivität die Verbindung automatisch getrennt wird. Hier sind Werte zwischen 60 und 300 Sekunden empfehlenswert. Wenn *Dial-On-Demand* deaktiviert ist, kann es hilfreich sein, das Zeitlimit auf Null zu setzen, um das automatische Trennen der Verbindung zu vermeiden.

Die Konfiguration von T-DSL erfolgt ähnlich wie die DSL-Konfiguration. Wählen Sie einfach *T-Online* als Provider und YaST öffnet das Konfigurationsdialogfeld für T-DSL. In diesem Dialogfeld geben Sie einige zusätzliche Informationen ein, die für

T-DSL erforderlich sind: die Anschlusskennung, die T-Online-Nummer, die Benutzerkennung und Ihr Passwort. Diese Informationen finden Sie in den T-DSL-Anmeldeunterlagen.

17.4.6 IBM-System z: Konfigurieren von Netzwerkgeräten

SUSE Linux Enterprise Server für IBM-System z unterstützt mehrere verschiedene Netzwerkschnittstellen. YaST kann zur Konfiguration dieser Schnittstellen verwendet werden.

Das qeth-hsi-Gerät

Wenn Sie dem installierten System eine `qeth-hsi`-Schnittstelle (IBM Hipersocket) hinzufügen möchten, starten Sie in YaST das Modul *Netzwerkgeräte* > *Netzwerkeinstellungen*. Wählen Sie eines der Geräte mit der Bezeichnung *Hipersocket* aus, um es als READ-Geräteadresse zu verwenden, und klicken Sie auf *Bearbeiten*. Geben Sie eine Gerätenummer für den Lesekanal, Schreibkanal und Steuerungskanal ein (Beispielformat für die Gerätenummer: 0.0.0600). Klicken Sie anschließend auf "Weiter". Im Dialogfeld *Konfiguration der Netzwerkadresse* geben Sie die IP-Adresse und die Netzmaske für die neue Schnittstelle an. Klicken Sie danach auf *Weiter* und *OK*, um die Netzwerkkonfiguration zu beenden.

Das qeth-ethernet-Gerät

Wenn Sie dem installierten System eine `qeth-ethernet`-Schnittstelle (IBM OSA Express Ethernet Card) hinzufügen möchten, starten Sie in YaST das Modul *Netzwerkgeräte* > *Netzwerkeinstellungen*. Wählen Sie eines der Geräte aus, die als *IBM OSA Express Ethernet Card* markiert sind, um es als READ zu verwenden. Geben Sie eine Gerätenummer für den Lesekanal, Schreibkanal und Steuerungskanal ein (Beispielformat für die Gerätenummer: 0.0.0600). Wählen Sie die Geräteadresse aus und klicken Sie auf *Bearbeiten*. Geben Sie den erforderlichen Portnamen, Portnummer (falls zutreffend), einige zusätzliche Optionen (siehe *Linux für IBM-System z*: Handbücher für Gerätetreiber, Funktionen und Kommandos als Referenz, `http://www.ibm.com/developerworks/linux/linux390/index.html`), Ihre IP-Adresse und eine entsprechende Netzmaske ein. Beenden Sie die Netzwerkkonfiguration mit *Weiter* und *OK*.

Das ctc-Gerät

Wenn Sie dem installierten System eine `ctc`-Schnittstelle (IBM Parallel CTC Adapter) hinzufügen möchten, starten Sie in YaST das Modul *Netzwerkgeräte* > *Netzwerkeinstellungen*. Wählen Sie eines der Geräte mit der Bezeichnung *IBM Parallel CTC Adapter* aus, um es als Lesekanal zu verwenden und klicken Sie auf *Konfigurieren*. Wählen Sie die *Geräteeinstellungen* für Ihre Geräte aus (gewöhnlich ist das *Kompatibilitätsmodus*). Geben Sie Ihre IP-Adresse und die IP-Adresse des entfernten Partners ein. Passen Sie gegebenenfalls die MTU-Größe mit *Erweitert* > *Besondere Einstellungen* an. Beenden Sie die Netzwerkkonfiguration mit *Weiter* und *OK*.

WARNUNG

Die Nutzung dieser Schnittstelle ist veraltet. Diese Schnittstelle wird in künftigen Versionen von SUSE Linux Enterprise Server nicht mehr unterstützt.

Das lcs-Gerät

Wenn Sie dem installierten System eine `lcs`-Schnittstelle (IBM OSA-2 Adapter) hinzufügen möchten, starten Sie in YaST das Modul *Netzwerkgeräte* > *Netzwerkeinstellungen*. Wählen Sie eines der Geräte mit der Bezeichnung *IBM OSA-2 Adapter* und klicken Sie auf *Konfigurieren*. Geben Sie die erforderliche Portnummer, einige zusätzliche Optionen (siehe *Linux für IBM-System z*: Handbücher für Gerätetreiber, Funktionen und Befehle als Referenz, `http://www.ibm.com/developerworks/linux/linux390/index.html`), Ihre IP-Adresse und eine entsprechende Netzmaske ein. Beenden Sie die Netzwerkkonfiguration mit *Weiter* und *OK*.

Das IUCV-Gerät

Wenn Sie dem installierten System eine `iucv`-Schnittstelle (IUCV) hinzufügen möchten, starten Sie in YaST das Modul *Netzwerkgeräte* > *Netzwerkeinstellungen*. Wählen Sie eines der Geräte mit der Bezeichnung *IUCV* und klicken Sie auf *Bearbeiten*. YaST fordert Sie auf, den Namen Ihres IUCV-Partners (*Peer*) einzugeben. Geben Sie den Namen ein (beachten Sie die Groß-/Kleinschreibung) und wählen Sie *Weiter*. Geben Sie Ihre *IP-Adresse* und die *Entfernte IP-Adresse* des Partners ein. Stellen Sie bei Bedarf die MTU-Größe über die Option *MTU festlegen* im Karteireiter *Allgemein* ein. Beenden Sie die Netzwerkkonfiguration mit *Weiter* und *OK*.

WARNUNG

Die Nutzung dieser Schnittstelle ist veraltet. Diese Schnittstelle wird in künftigen Versionen von SUSE Linux Enterprise Server nicht mehr unterstützt.

17.5 NetworkManager

NetworkManager ist die ideale Lösung für einen mobilen Arbeitsplatzrechner. Wenn Sie viel unterwegs sind und den NetworkManager verwenden, brauchen Sie keine Gedanken mehr an die Konfiguration von Netzwerkschnittstellen und den Wechsel zwischen Netzwerken zu verschwenden. NetworkManager kann automatisch Verbindungen zu den bekannten WLAN-Netzwerken herstellen. Bei zwei oder gar mehreren Verbindungsmöglichkeiten stellt der NetworkManager die Verbindung zum schnelleren Netzwerk her.

NetworkManager ist jedoch nicht in jedem Fall eine passende Lösung, daher können Sie immer noch zwischen der herkömmlichen Methode zur Verwaltung von Netzwerkverbindungen (ifup) und NetworkManager wählen. Wenn Ihre Netzwerkverbindung mit NetworkManager verwaltet werden soll, aktivieren Sie NetworkManager im Netzwerkeinstellungsmodul von YaST wie in Abschnitt 23.2, „Aktivieren von NetworkManager“ (S. 360) beschrieben und konfigurieren Sie Ihre Netzwerkverbindungen mit NetworkManager. Eine Liste der Anwendungsfälle sowie eine detaillierte Beschreibung zur Konfiguration und Verwendung von NetworkManager finden Sie unter Kapitel 23, *Verwenden von NetworkManager* (S. 359).

Einige Unterschiede zwischen ifup und NetworkManager sind:

`root`-Berechtigungen
: Wenn Sie NetworkManager zur Netzwerkeinrichtung verwenden, können Sie mithilfe eines Miniprogramms von Ihrer Desktop-Umgebung aus Ihre Netzwerkverbindung jederzeit auf einfache Weise wechseln, stoppen oder starten. NetworkManager ermöglicht zudem die Änderung und Konfiguration drahtloser Kartenverbindungen ohne Anforderung von `root`-Berechtigungen. Aus diesem Grund ist NetworkManager die ideale Lösung für einen mobilen Arbeitsplatzrechner.

  Die herkömmliche Konfiguration mit ifup bietet wie die benutzerverwalteten Geräte ebenfalls verschiedene Möglichkeiten zum Wechseln, Stoppen oder Starten der Verbindung mit oder ohne Benutzereingriff. Jedoch sind `root`-Berechtigungen

erforderlich, um ein Netzwerkgerät zu ändern oder zu konfigurieren. Dies stellt häufig ein Problem bei der mobilen Computernutzung dar, bei der es nicht möglich ist, alle Verbindungsmöglichkeiten vorzukonfigurieren.

Typen von Netzwerkverbindungen
: Sowohl die herkömmliche Konfiguration als auch NetworkManager können Netzwerkverbindungen mit drahtlosen Netzwerken (mit WEP-, WPA-PSK- und WPA-Enterprise-Zugriff), Einwahlverbindungen und verkabelten Netzwerken herstellen und dabei DHCP oder statische Konfigurationen verwenden. Darüber hinaus unterstützen sie Verbindungen über VPN.

  NetworkManager sorgt für eine zuverlässige Verbindung rund um die Uhr und verwendet dazu die beste verfügbare Verbindung. Wurde das Netzwerkkabel versehentlich ausgesteckt, wird erneut versucht, eine Verbindung herzustellen. Der NetworkManager sucht in der Liste Ihrer drahtlosen Verbindungen nach dem Netzwerk mit dem stärksten Signal und stellt automatisch eine Verbindung her. Wenn Sie dieselbe Funktionalität mit ifup erhalten möchten, ist einiger Konfigurationsaufwand erforderlich.

17.6 Manuelle Netzwerkkonfiguration

Die manuelle Konfiguration der Netzwerksoftware sollte immer die letzte Alternative sein. Wir empfehlen, YaST zu benutzen. Die folgenden Hintergrundinformationen zur Netzwerkkonfiguration können Ihnen jedoch auch bei der Arbeit mit YaST behilflich sein.

Wenn der Kernel eine Netzwerkkarte erkennt und eine entsprechende Netzwerkschnittstelle erstellt, weist er dem Gerät einen Namen zu. Dieser richtet sich nach der Reihenfolge der Geräteerkennung bzw. nach der Reihenfolge, in der die Kernel-Module geladen werden. Die vom Kernel vergebenen Standardgerätenamen lassen sich nur in sehr einfachen oder überaus kontrollierten Hardwareumgebungen vorhersagen. Auf Systemen, auf denen es möglich ist, Hardware während der Laufzeit hinzuzufügen oder zu entfernen, oder die die automatische Konfiguration von Geräten zulassen, können vom Kernel über mehrere Neustarts hinaus keine stabilen Netzwerkgerätenamen erwartet werden.

Für die Systemkonfigurationstools sind jedoch dauerhafte (persistente) Schnittstellennamen erforderlich. Dieses Problem wird durch udev gelöst. Der udev-persistente Netzgenerator (`/etc/udev/rules.d/75-persistent-net-generator`

.rules) generiert eine Regel für den Hardwareabgleich (standardmäßig mit seiner Hardwareadresse) und weist eine dauerhaft eindeutige Schnittstelle für die Hardware zu. Die udev-Datenbank mit den Netzwerkschnittstellen wird in der Datei /etc/udev/rules.d/70-persistent-net.rules gespeichert. Pro Zeile dieser Datei wird eine Netzwerkschnittstelle beschrieben und deren persistenter Name angegeben. Die zugewiesenen Namen können vom Systemadministrator im Eintrag NAME="" geändert werden. Die persistenten Regeln können auch mithilfe von YaST geändert werden.

Tabelle 17.5, „Skripten für die manuelle Netzwerkkonfiguration“ (S. 268) zeigt die wichtigsten an der Netzwerkkonfiguration beteiligten Skripten.

Tabelle 17.5 *Skripten für die manuelle Netzwerkkonfiguration*

Befehl	Funktion
if{up,down,status}	Die if*-Skripten starten oder stoppen Netzwerkschnittstellen oder geben den Status der angegebenen Schnittstelle zurück. Weitere Informationen hierzu finden Sie auf der Manualpage für den Befehl ifup.
rcnetwork	Mit dem Skript rcnetwork können alle Netzwerkschnittstellen oder nur eine bestimmte Netzwerkschnittstelle gestartet, gestoppt oder neu gestartet werden. Verwenden Sie rcnetwork stop zum Anhalten, rcnetwork start zum Starten und rcnetwork restart zum Neustart von Netzwerkschnittstellen. Wenn Sie nur eine Netzwerkschnittstelle stoppen, starten oder neu starten möchten, geben Sie nach dem jeweiligen Kommando den Namen der Schnittstelle ein, zum Beispiel rcnetwork restart eth0. Das Kommando rcnetwork status zeigt den Status und die IP-Adressen der Netzwerkschnittstellen an. Außerdem gibt das Kommando an, ob auf den Schnittstellen ein DHCP-Client ausgeführt wird. Mit rcnetwork stop-all-dhcp-clients und rcnetwork restart-all-dhcp-clients können Sie die auf den Netzwerkschnittstellen ausgeführten DHCP-Clients stoppen und wieder starten.

Weitere Informationen zu udev und persistenten Gerätenamen finden Sie in Kapitel 11, *Gerätemanagemet über dynamischen Kernel mithilfe von udev* (S. 143).

17.6.1 Konfigurationsdateien

Dieser Abschnitt bietet einen Überblick über die Netzwerkkonfigurationsdateien und erklärt ihren Zweck sowie das verwendete Format.

/etc/sysconfig/network/ifcfg-*

Diese Dateien enthalten die Konfigurationsdaten für Netzwerkschnittstellen. Sie enthalten Informationen wie den Startmodus und die IP-Adresse. Mögliche Parameter sind auf der man-Seite für den Befehl `ifup` beschrieben. Wenn nur eine einzelne allgemeine Einstellung nur für eine bestimmte Schnittstelle verwendet werden soll, können außerdem alle Variablen aus den Dateien `dhcp`, `wireless` und `config` in den `ifcfg-*`-Dateien verwendet werden.

► **zseries:** IBM-System z unterstützen USB nicht. Die Namen der Schnittstellendateien und Netzwerkaliasse enthalten System z-spezifische Elemente wie `qeth`. ◄

/etc/sysconfig/network/{config, dhcp, wireless}

Die Datei `config` enthält allgemeine Einstellungen für das Verhalten von `ifup`, `ifdown` und `ifstatus`. `dhcp` enthält DHCP-Einstellungen und `wireless` Einstellungen für Wireless-LAN-Karten. Die Variablen in allen drei Konfigurationsdateien sind kommentiert. Einige der Variablen von `/etc/sysconfig/network/config` können auch in `ifcfg-*`-Dateien verwendet werden, wo sie mit höherer Priorität behandelt werden. Die Datei `/etc/sysconfig/network/ifcfg.template` listet Variablen auf, die mit einer Reichweite pro Schnittstelle angegeben werden können. Jedoch sind die meisten `/etc/sysconfig/network/config`-Variablen global und lassen sich in ifcfg-Dateien nicht überschreiben. Beispielsweise sind die Variablen `NETWORKMANAGER` oder `NETCONFIG_*` global.

/etc/sysconfig/network/{routes,ifroute-*}

Hier wird das statische Routing von TCP/IP-Paketen festgelegt. Alle statischen Routen, die für verschiedenen Systemaufgaben benötigt werden, können in die Datei `/etc/sysconfig/network/routes` eingegeben werden: Routen zu einem Host, Routen zu einem Host über Gateways und Routen zu einem Netzwerk. Definieren Sie für jede Schnittstelle, die individuelles Routing benötigt, eine zusätzliche Konfigurationsdatei: `/etc/sysconfig/network/ifroute-*`. Ersetzen Sie `*` durch den Namen der Schnittstelle. Die folgenden Einträge werden in die Routing-Konfigurationsdatei aufgenommen:

```
# Destination     Dummy/Gateway     Netmask            Device
#
127.0.0.0         0.0.0.0           255.255.255.0      lo
204.127.235.0     0.0.0.0           255.255.255.0      eth0
default           204.127.235.41    0.0.0.0            eth0
207.68.156.51     207.68.145.45     255.255.255.255    eth1
192.168.0.0       207.68.156.51     255.255.0.0        eth1
```

Das Routenziel steht in der ersten Spalte. Diese Spalte kann die IP-Adresse eines Netzwerks oder Hosts bzw., im Fall von *erreichbaren* Namenservern, den voll qualifizierten Netzwerk- oder Hostnamen enthalten.

Die zweite Spalte enthält das Standard-Gateway oder ein Gateway, über das der Zugriff auf einen Host oder ein Netzwerk erfolgt. Die dritte Spalte enthält die Netzmaske für Netzwerke oder Hosts hinter einem Gateway. Die Maske `255.255.255.255` gilt beispielsweise für einen Host hinter einem Gateway.

Die vierte Spalte ist nur für Netzwerke relevant, die mit dem lokalen Host verbunden sind, z. B. Loopback-, Ethernet-, ISDN-, PPP- oder Dummy-Geräte. In diese Spalte muss der Gerätename eingegeben werden.

In einer (optionalen) fünften Spalte kann der Typ einer Route angegeben werden. Nicht benötigte Spalten sollten ein Minuszeichen – enthalten, um sicherzustellen, dass der Parser den Befehl korrekt interpretiert. Weitere Informationen hierzu finden Sie auf der Manualpage für den Befehl `routes(5)`.

/etc/resolv.conf

In dieser Datei wird die Domäne angegeben, zu der der Host gehört (Schlüsselwort `search`). Ebenfalls aufgeführt ist der Status des Namenservers, auf den der Zugriff

erfolgt (Schlüsselwort `nameserver`). In der Datei können mehrere Domänennamen angegeben werden. Bei der Auflösung eines Namens, der nicht voll qualifiziert ist, wird versucht, einen solchen zu generieren, indem die einzelnen `search`-Einträge angehängt werden. Mehrere Namenserver können in mehreren Zeilen angegeben werden, von denen jede mit `nameserver` beginnt. Kommentaren werden #-Zeichen vorangestellt. Beispiel 17.5, „`/etc/resolv.conf`“ (S. 271) zeigt, wie `/etc/resolv.conf` aussehen könnte.

Jedoch darf `/etc/resolv.conf` nicht manuell bearbeitet werden. Stattdessen wird es vom Skript `netconfig` generiert. Bearbeiten Sie zum Definieren der statischen DNS-Konfiguration ohne YaST manuell die entsprechenden Variablen in der Datei `/etc/sysconfig/network/config`: `NETCONFIG_DNS_STATIC_SEARCHLIST` (Liste von DNS-Domänennamen für die Suche nach Hostnamen), `NETCONFIG_DNS_STATIC_SERVERS` (Liste von Namenserver-IP-Adressen für die Suche nach Hostnamen), `NETCONFIG_DNS_FORWARDER` (definiert den Namen des DNS-Forwarder, der konfiguriert werden muss). Zum Deaktivieren der DNS-Konfiguration mit netconfig setzen Sie `NETCONFIG_DNS_POLICY=''`. Weitere Informationen über `netconfig` finden Sie auf `man 8 netconfig`.

Beispiel 17.5 */etc/resolv.conf*

```
# Our domain
search example.com
#
# We use dns.example.com (192.168.1.116) as nameserver
nameserver 192.168.1.116
```

/sbin/netconfig

`netconfig` ist ein modulares Tool zum Verwalten zusätzlicher Netzwerkkonfigurationseinstellungen. Es führt statisch definierte Einstellungen mit Einstellungen zusammen, die von automatischen Konfigurationsmechanismen wie dhcp oder ppp gemäß einer vordefinierten Richtlinie bereitgestellt wurden. Die erforderlichen Änderungen werden dem System zugewiesen, indem die netconfig-Module aufgerufen werden, die für das Ändern einer Konfigurationsdatei und den Neustart eines Service oder eine ähnliche Aktion verantwortlich sind.

`netconfig` erkennt drei Hauptaktionen. Die Kommandos `netconfig modify` und `netconfig remove` werden von Daemons wie dhcp oder ppp verwendet, um

Einstellungen für netconfig hinzuzufügen oder zu entfernen. Nur das Kommando `netconfig update` steht dem Benutzer zur Verfügung:

`modify`
: Das Kommando `netconfig modify` ändert die aktuelle Schnittstellen- und Service-spezifischen dynamischen Einstellungen und aktualisiert die Netzwerkkonfiguration. Netconfig liest Einstellungen aus der Standardeingabe oder einer Datei, die mit der Option `--lease-file` *`Dateiname`* angegeben wurde, und speichert sie intern bis zu einem System-Reboot oder der nächsten Änderungs- oder Löschaktion. Bereits vorhandene Einstellungen für dieselbe Schnittstellen- und Service-Kombination werden überschrieben. Die Schnittstelle wird durch den Parameter `-i` *`Schnittstellenname`* angegeben. Der Service wird durch den Parameter `-s` *`Servicename`* angegeben.

`Entfernen`
: Das Kommando `netconfig remove` entfernt die dynamischen Einstellungen, die von einer Änderungsaktion für die angegebene Schnittstellen- und Service-Kombination bereitgestellt wurden, und aktualisiert die Netzwerkkonfiguration. Die Schnittstelle wird durch den Parameter `-i` *`Schnittstellenname`* angegeben. Der Service wird durch den Parameter `-s` *`Servicename`* angegeben.

`Aktualisieren`
: Das Kommando `netconfig update` aktualisiert die Netzwerkkonfiguration mit den aktuellen Einstellungen. Dies ist nützlich, wenn sich die Richtlinie oder die statische Konfiguration geändert hat.

Die Einstellungen für die netconfig-Richtlinie und die statische Konfiguration werden entweder manuell oder mithilfe von YaST in der Datei `/etc/sysconfig/network/config` definiert. Die dynamischen Konfigurationseinstellungen von Tools zur automatischen Konfiguration wie dhcp oder ppp werden von diesen Tools mit den Aktionen `netconfig modify` und `netconfig remove` direkt bereitgestellt. NetworkManager verwendet auch die Aktionen `netconfig modify` und `netconfig remove`. Wenn NetworkManager aktiviert ist, verwendet netconfig (im Richtlinienmodus `auto`) nur NetworkManager-Einstellungen und ignoriert Einstellungen von allen anderen Schnittstellen, die mit der traditionellen ifup-Methode konfiguriert wurden. Wenn NetworkManager keine Einstellung liefert, werden als Fallback statische Einstellungen verwendet. Eine gemischte Verwendung von NetworkManager und der traditionellen ifup-Methode wird nicht unterstützt.

Weitere Informationen über `netconfig` finden Sie auf `man 8 netconfig`.

/etc/hosts

In dieser Datei werden, wie in Beispiel 17.6, „`/etc/hosts`“ (S. 273) gezeigt, IP-Adressen zu Hostnamen zugewiesen. Wenn kein Namenserver implementiert ist, müssen alle Hosts, für die IP-Verbindungen eingerichtet werden sollen, hier aufgeführt sein. Geben Sie für jeden Host in die Datei eine Zeile ein, die aus der IP-Adresse, dem voll qualifizierten Hostnamen und dem Hostnamen besteht. Die IP-Adresse muss am Anfang der Zeile stehen und die Einträge müssen durch Leerzeichen und Tabulatoren getrennt werden. Kommentaren wird immer das #-Zeichen vorangestellt.

Beispiel 17.6 */etc/hosts*

```
127.0.0.1 localhost
192.168.2.100 jupiter.example.com jupiter
192.168.2.101 venus.example.com venus
```

/etc/networks

Hier werden Netzwerknamen in Netzwerkadressen umgesetzt. Das Format ähnelt dem der `hosts`-Datei, jedoch stehen hier die Netzwerknamen vor den Adressen. Weitere Informationen hierzu finden Sie unter Beispiel 17.7, „`/etc/networks`“ (S. 273).

Beispiel 17.7 */etc/networks*

```
loopback     127.0.0.0
localnet     192.168.0.0
```

/etc/host.conf

Diese Datei steuert das Auflösen von Namen, d. h. das Übersetzen von Host- und Netzwerknamen über die *resolver*-Bibilothek. Diese Datei wird nur für Programme verwendet, die mit libc4 oder libc5 gelinkt sind. Weitere Informationen zu aktuellen glibc-Programmen finden Sie in den Einstellungen in `/etc/nsswitch.conf`. Jeder Parameter muss in einer eigenen Zeile stehen. Kommentare werden durch ein #-Zeichen eingeleitet. Die verfügbaren Parameter sind in Tabelle 17.6, „Parameter für /etc/host.conf“ (S. 274) aufgeführt. Ein Beispiel für `/etc/host.conf` wird in Beispiel 17.8, „`/etc/host.conf`“ (S. 274) gezeigt.

Tabelle 17.6 *Parameter für /etc/host.conf*

order *hosts*, *bind*	Legt fest, in welcher Reihenfolge die Dienste zum Auflösen eines Namens angesprochen werden sollen. Mögliche Argumente (getrennt durch Leerzeichen oder Kommas): *Hosts*: Sucht die `/etc/hosts`-Datei *bind*: Greift auf einen Namenserver zu *nis*: Verwendet NIS
multi *on*/*off*	Legt fest, ob ein in `/etc/hosts` eingegebener Host mehrere IP-Adressen haben kann.
nospoof *on* spoofalert *on*/*off*	Diese Parameter beeinflussen das *spoofing* des Namenservers, haben aber keinen Einfluss auf die Netzwerkkonfiguration.
trim *Domänenname*	Der angegebene Domänenname wird vor dem Auflösen des Hostnamens von diesem abgeschnitten (insofern der Hostname diesen Domänennamen enthält). Diese Option ist dann von Nutzen, wenn in der Datei `/etc/hosts` nur Namen aus der lokalen Domäne stehen, diese aber auch mit angehängtem Domänennamen erkannt werden sollen.

Beispiel 17.8 */etc/host.conf*

```
# We have named running
order hosts bind
# Allow multiple address
multi on
```

/etc/nsswitch.conf

Mit der GNU C Library 2.0 wurde *Name Service Switch* (NSS) eingeführt. Weitere Informationen hierzu finden Sie auf der Manualpage für `nsswitch.conf(5)` und im Dokument *The GNU C Library Reference Manual.*

In der Datei `/etc/nsswitch.conf` wird festgelegt, in welcher Reihenfolge bestimmte Informationen abgefragt werden. Ein Beispiel für `nsswitch.conf` ist in

Beispiel 17.9, „/etc/nsswitch.conf“ (S. 275) dargestellt. Kommentare werden durch ein #-Zeichen eingeleitet. Der Eintrag unter der hosts-Datenbank bedeutet, dass Anfragen über DNS an /etc/hosts (files) gehen (siehe Kapitel 21, *Domain Name System (DNS)* (S. 313)).

Beispiel 17.9 */etc/nsswitch.conf*

```
passwd:     compat
group:      compat

hosts:      files dns
networks:   files dns

services:   db files
protocols:  db files

netgroup:   files
automount:  files nis
```

Die über NSS verfügbaren "Datenbanken" sind in Tabelle 17.7, „Über /etc/nsswitch.conf verfügbare Datenbanken“ (S. 275) aufgelistet. Zusätzlich sind in Zukunft zudem automount, bootparams, netmasks und publickey zu erwarten. Die Konfigurationsoptionen für NSS-Datenbanken sind in Tabelle 17.8, „Konfigurationsoptionen für NSS-"Datenbanken"“ (S. 276) aufgelistet.

Tabelle 17.7 *Über /etc/nsswitch.conf verfügbare Datenbanken*

aliases	Mail-Aliasse, die von sendmail implementiert werden. Siehe man5 aliases.
ethers	Ethernet-Adressen
Gruppe	Für Benutzergruppen, die von getgrent verwendet werden. Weitere Informationen hierzu finden Sie auch auf der Manualpage für den Befehl group.
hosts	Für Hostnamen und IP-Adressen, die von gethostbyname und ähnlichen Funktionen verwendet werden.
netgroup	Im Netzwerk gültige Host- und Benutzerlisten zum Steuern von Zugriffsrechten. Weitere Informationen hierzu finden Sie auf der Manualpage für netgroup(5).

`networks`	Netzwerknamen und -adressen, die von `getnetent` verwendet werden.
`passwd`	Benutzerpasswörter, die von `getpwent` verwendet werden. Weitere Informationen hierzu finden Sie auf der Manualpage `passwd(5)`.
`protocols`	Netzwerkprotokolle, die von `getprotoent` verwendet werden. Weitere Informationen hierzu finden Sie auf der Manualpage für `protocols(5)`.
`rpc`	Remote Procedure Call-Namen und -Adressen, die von `getrpcbyname` und ähnlichen Funktionen verwendet werden.
`services`	Netzwerkdienste, die von `getservent` verwendet werden.
`shadow`	Shadow-Passwörter der Benutzer, die von `getspnam` verwendet werden. Weitere Informationen hierzu finden Sie auf der Manualpage für `shadow(5)`.

Tabelle 17.8 *Konfigurationsoptionen für NSS-"Datenbanken"*

`Dateien`	Direkter Dateizugriff, z. B. `/etc/aliases`
`db`	Zugriff über eine Datenbank
`nis`, `nisplus`	NIS, siehe auch Kapitel 4, *Using NIS* (↑*Security Guide*)
`dns`	Nur bei `hosts` und `networks` als Erweiterung verwendbar
`compat`	Nur bei `passwd`, `shadow` und `group` als Erweiterung verwendbar

/etc/nscd.conf

Mit dieser Datei wird nscd (Name Service Cache Daemon) konfiguriert. Weitere Informationen hierzu finden Sie auf den man-Seiten `nscd(8)` und `nscd.conf(5)`. Standardmäßig werden die Systemeinträge von `passwd` und `groups` von nscd gecacht. Dies ist wichtig für die Leistung der Verzeichnisdienste, z. B. NIS und LDAP, da anderenfalls die Netzwerkverbindung für jeden Zugriff auf Namen oder Gruppen verwendet werden muss. `hosts` wird standardmäßig nicht gecacht, da der Mechanismus in nscd dazu führen würde, dass das lokale System keine Trust-Forward- und Reverse-Lookup-Tests mehr ausführen kann. Statt nscd das Cachen der Namen zu übertragen, sollten Sie einen DNS-Server für das Cachen einrichten.

Wenn das Caching für `passwd` aktiviert wird, dauert es in der Regel 15 Sekunden, bis ein neu angelegter lokaler Benutzer dem System bekannt ist. Durch das Neustarten von nscd mit dem Befehl `rcnscd restart` kann diese Wartezeit verkürzt werden.

/etc/HOSTNAME

Hier steht der Name des Computers, also nur der Hostname ohne den Domänennamen. Diese Datei wird von verschiedenen Skripten beim Booten des Computers gelesen. Sie darf nur eine Zeile enthalten, in der der Hostname steht.

17.6.2 Testen der Konfiguration

Bevor Sie Ihre Konfiguration in den Konfigurationsdateien speichern, können Sie sie testen. Zum Einrichten einer Testkonfiguration verwenden Sie den Befehl `ip`. Zum Testen der Verbindung verwenden Sie den Befehl `ping`. Ältere Konfigurationswerkzeuge, `ifconfig` und `route`, sind ebenfalls verfügbar.

Die Befehle `ip`, `ifconfig` und `route` ändern die Netzwerkkonfiguration direkt, ohne sie in der Konfigurationsdatei zu speichern. Wenn Sie die Konfiguration nicht in die korrekten Konfigurationsdateien eingeben, geht die geänderte Netzwerkkonfiguration nach dem Neustart verloren.

Konfigurieren einer Netzwerkschnittstelle mit ip

`ip` ist ein Werkzeug zum Anzeigen und Konfigurieren von Routing, Netzwerkgeräten, Richtlinien-Routing und Tunneln. Er wurde als Ersatz für die älteren Werkzeuge ifconfig und route gedacht.

`ip` ist ein sehr komplexes Werkzeug. Seine allgemeine Syntax ist `ip` *`options object command`*. Sie können mit folgenden Objekten arbeiten:

Verbindung
: Dieses Objekt stellt ein Netzwerkgerät dar.

Adresse
: Dieses Objekt stellt die IP-Adresse des Geräts dar.

neighbour
: Dieses Objekt stellt einen ARP- oder NDISC-Cache-Eintrag dar.

route
: Dieses Objekt stellt den Routing-Tabelleneintrag dar.

Regel
: Dieses Objekt stellt eine Regel in der Routing-Richtlinien-Datenbank dar.

maddress
: Dieses Objekt stellt eine Multicast-Adresse dar.

mroute
: Dieses Objekt stellt einen Multicast-Routing-Cache-Eintrag dar.

tunnel
: Dieses Objekt stellt einen Tunnel über IP dar.

Wird kein Befehl angegeben, wird der Standardbefehl verwendet. Normalerweise ist das `list`.

Ändern Sie den Gerätestatus mit dem Befehl `ip link set` *`device_name command`*. Wenn Sie beispielsweise das Gerät eth0 deaktivieren möchten, geben Sie `ip link seteth0 down ein`. Um es wieder zu aktivieren, verwenden Sie `ip link seteth0 up`.

Nach dem Aktivieren eines Geräts können Sie es konfigurieren. Verwenden Sie zum Festlegen der IP-Adresse `ip addr add`*`ip_address`* `+ dev` *`device_name`*. Wenn Sie beispielsweise die Adresse der Schnittstelle eth0 mit dem standardmäßigen Broadcast (Option `brd`) auf 192.168.12.154/30 einstellen möchten, geben Sie `ip addr add 192.168.12.154/30 brd + dev eth0` ein.

Damit die Verbindung funktioniert, müssen Sie außerdem das Standard-Gateway konfigurieren. Geben Sie `ip route add gateway_ip_address` ein, wenn Sie ein Gateway für Ihr System festlegen möchten. Um eine IP-Adresse in eine andere Adresse zu übersetzen, verwenden Sie `nat: ip route add nat ip_address via other_ip_address`.

Zum Anzeigen aller Geräte verwenden Sie `ip link ls`. Wenn Sie nur die aktiven Schnittstellen abrufen möchten, verwenden Sie `ip link ls up`. Um Schnittstellenstatistiken für ein Gerät zu drucken, geben Sie `ip -s link lsdevice_name` ein. Um die Adressen Ihrer Geräte anzuzeigen, geben Sie `ip addr` ein. In der Ausgabe von `ip addr` finden Sie auch Informationen zu MAC-Adressen Ihrer Geräte. Wenn Sie alle Routen anzeigen möchten, wählen Sie `ip route show`.

Weitere Informationen zur Verwendung von ip erhalten Sie, indem Sie `iphelp` eingeben oder die man-Seite `ip(8)` aufrufen. Die Option `help` ist zudem für alle ip-Objekte verfügbar. Wenn Sie beispielsweise Hilfe zu `ipaddr` benötigen, geben Sie `ipaddr help` ein. Suchen Sie die IP-Manualpage in der Datei `/usr/share/doc/packages/iproute2/ip-cref.pdf`.

Testen einer Verbindung mit ping

Der `ping`-Befehl ist das Standardwerkzeug zum Testen, ob eine TCP/IP-Verbindung funktioniert. Er verwendet das ICMP-Protokoll, um ein kleines Datenpaket, das ECHO_REQUEST-Datagram, an den Ziel-Host zu senden. Dabei wird eine sofortige Antwort angefordert. Funktioniert dies, erhalten Sie eine Meldung, die Ihnen bestätigt, dass die Netzwerkverbindung grundsätzlich funktioniert.

`ping` testet nicht nur die Funktion der Verbindung zwischen zwei Computern, es bietet darüber hinaus grundlegende Informationen zur Qualität der Verbindung. In Beispiel 17.10, „Ausgabe des ping-Befehls“ (S. 280) sehen Sie ein Beispiel der `ping`-Ausgabe. Die vorletzte Zeile enthält Informationen zur Anzahl der übertragenen Pakete, der verlorenen Pakete und der Gesamtlaufzeit von `ping`.

Als Ziel können Sie einen Hostnamen oder eine IP-Adresse verwenden, z. B. `ping example.com` oder `ping 192.168.3.100`. Das Programm sendet Pakete, bis Sie auf Strg + C drücken.

Wenn Sie nur die Funktion der Verbindung überprüfen möchten, können Sie die Anzahl der Pakete durch die Option `-c` beschränken. Wenn die Anzahl beispielsweise auf drei Pakete beschränkt werden soll, geben Sie `ping -c 3 example.com` ein.

Beispiel 17.10 *Ausgabe des ping-Befehls*

```
ping -c 3 example.com
PING example.com (192.168.3.100) 56(84) bytes of data.
64 bytes from example.com (192.168.3.100): icmp_seq=1 ttl=49 time=188 ms
64 bytes from example.com (192.168.3.100): icmp_seq=2 ttl=49 time=184 ms
64 bytes from example.com (192.168.3.100): icmp_seq=3 ttl=49 time=183 ms
--- example.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2007ms
rtt min/avg/max/mdev = 183.417/185.447/188.259/2.052 ms
```

Das Standardintervall zwischen zwei Paketen beträgt eine Sekunde. Zum Ändern des Intervalls bietet der ping-Befehl die Option `-i`. Wenn beispielsweise das Ping-Intervall auf zehn Sekunden erhöht werden soll, geben Sie `ping -i 10 example.com` ein.

In einem System mit mehreren Netzwerkgeräten ist es manchmal nützlich, wenn der ping-Befehl über eine spezifische Schnittstellenadresse gesendet wird. Verwenden Sie hierfür die Option `-I` mit dem Namen des ausgewählten Geräts. Beispiel: `ping -I wlan1 example.com`.

Weitere Optionen und Informationen zur Verwendung von ping erhalten Sie, indem Sie `ping-h` eingeben oder die man-Seite `ping (8)` aufrufen.

Konfigurieren des Netzwerks mit dem ifconfig-Befehl

`ifconfig` ist ein herkömmliches Werkzeug zur Netzwerkkonfiguration. Im Gegensatz zu ip, können Sie diesen Befehl nur für die Schnittstellenkonfiguration verwenden. Das Routing konfigurieren Sie mit `route`.

ANMERKUNG: ifconfig und ip

Das ifconfig-Programm ist veraltet. Verwenden Sie stattdessen ip.

Ohne Argumente zeigt ifconfig den Status der gegenwärtig aktiven Schnittstellen an. Unter Beispiel 17.11, „Ausgabe des ifconfig-Befehls“ (S. 281) sehen Sie, dass ifconfig über eine gut angeordnete, detaillierte Ausgabe verfügt. Die Ausgabe enthält außerdem in der ersten Zeile Informationen zur MAC-Adresse Ihres Geräts, dem Wert von `HWaddr`.

Beispiel 17.11 *Ausgabe des ifconfig-Befehls*

```
eth0      Link encap:Ethernet  HWaddr 00:08:74:98:ED:51
          inet6 addr: fe80::208:74ff:fe98:ed51/64 Scope:Link
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:634735 errors:0 dropped:0 overruns:4 frame:0
          TX packets:154779 errors:0 dropped:0 overruns:0 carrier:1
          collisions:0 txqueuelen:1000
          RX bytes:162531992 (155.0 Mb)  TX bytes:49575995 (47.2 Mb)
          Interrupt:11 Base address:0xec80

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:8559 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8559 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:533234 (520.7 Kb)  TX bytes:533234 (520.7 Kb)

wlan1     Link encap:Ethernet  HWaddr 00:0E:2E:52:3B:1D
          inet addr:192.168.2.4  Bcast:192.168.2.255  Mask:255.255.255.0
          inet6 addr: fe80::20e:2eff:fe52:3b1d/64 Scope:Link
          UP BROADCAST NOTRAILERS RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:50828 errors:0 dropped:0 overruns:0 frame:0
          TX packets:43770 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:45978185 (43.8 Mb)  TX bytes:7526693 (7.1 MB)
```

Weitere Optionen und Informationen zur Verwendung von `ifconfig` erhalten Sie, wenn Sie ifconfig-h eingeben oder die man-Seite `ifconfig (8)` aufrufen.

Konfigurieren des Routing mit route

`route` ist ein Programm zum Ändern der IP-Routing-Tabelle. Sie können damit Ihre Routing-Konfiguration anzeigen und Routen hinzufügen oder entfernen.

ANMERKUNG: route und ip

Das route-Programm ist veraltet. Verwenden Sie stattdessen ip.

route ist vor allem dann nützlich, wenn Sie schnelle und übersichtliche Informationen zu Ihrer Routing-Konfiguration benötigen, um Routing-Probleme zu ermitteln. Sie sehen Ihre aktuelle Routing-Konfiguration unter `route -n` als `root`.

Beispiel 17.12 *Ausgabe des route -n-Befehls*

```
route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
10.20.0.0       *               255.255.248.0   U         0 0          0 eth0
link-local      *               255.255.0.0     U         0 0          0 eth0
loopback        *               255.0.0.0       U         0 0          0 lo
default         styx.exam.com   0.0.0.0         UG        0 0          0 eth0
```

Weitere Optionen und Informationen zur Verwendung von `route` erhalten Sie, indem Sie `v-h` eingeben oder die man-Seite `route (8)` aufrufen.

17.6.3 Startup-Skripten

Neben den beschriebenen Konfigurationsdateien gibt es noch verschiedene Skripten, die beim Booten des Computers die Netzwerkprogramme starten. Diese werden gestartet, sobald das System in einen der *Mehrbenutzer-Runlevel* wechselt. Einige der Skripten sind in Tabelle 17.9, „Einige Start-Skripten für Netzwerkprogramme“ (S. 282) beschrieben.

Tabelle 17.9 *Einige Start-Skripten für Netzwerkprogramme*

`/etc/init.d/network`	Dieses Skript übernimmt die Konfiguration der Netzwerkschnittstellen. Wenn der `Netzwerkdienst` nicht gestartet wurde, werden keine Netzwerkschnittstellen implementiert.
`/etc/init.d/xinetd`	Startet xinetd. Mit xinetd können Sie Serverdienste auf dem System verfügbar machen. Beispielsweise kann er vsftpd starten, sobald eine FTP-Verbindung initiiert wird.
`/etc/init.d/portmap`	Startet den Portmapper, der für einen RPC-Server benötigt wird, z. B. für einen NFS-Server.

`/etc/init.d/nfsserver`	Startet den NFS-Server.
`/etc/init.d/postfix`	Steuert den postfix-Prozess.
`/etc/init.d/ypserv`	Startet den NIS-Server.
`/etc/init.d/ypbind`	Startet den NIS-Client.

17.7 smpppd als Einwählhelfer

Einige Heimanwender besitzen keine gesonderte Leitung für das Internet, sondern wählen sich bei Bedarf ein. Je nach Einwählart (ISDN oder DSL) wird die Verbindung von ipppd oder pppd gesteuert. Im Prinzip müssen nur diese Programme korrekt gestartet werden, um online zu sein.

Sofern Sie über eine Flatrate verfügen, die bei der Einwahl keine zusätzlichen Kosten verursacht, starten Sie einfach den entsprechenden Daemon. Sie können die Einwählverbindung über ein KDE-Applet oder eine Kommandozeilen-Schnittstelle steuern. Wenn das Internet-Gateway nicht der eigentliche Arbeitscomputer ist, besteht die Möglichkeit, die Einwählverbindung über einen Host im Netzwerk zu steuern.

An dieser Stelle kommt smpppd ins Spiel. Der Dienst bietet den Hilfsprogrammen eine einheitliche Schnittstelle, die in zwei Richtungen funktioniert. Zum einen programmiert er den jeweils erforderlichen pppd oder ipppd und steuert deren Einwählverhalten. Zum anderen stellt er den Benutzerprogrammen verschiedene Provider zur Verfügung und übermittelt Informationen zum aktuellen Status der Verbindung. Da der smpppd-Dienst auch über das Netzwerk gesteuert werden kann, eignet er sich für die Steuerung von Einwählverbindungen ins Internet von einer Arbeitsstation in einem privaten Subnetzwerk.

17.7.1 Konfigurieren von smpppd

Die von smpppd bereitgestellten Verbindungen werden automatisch von YaST konfiguriert. Die eigentlichen Einwählprogramme KInternet und cinternet werden ebenfalls vorkonfiguriert. Manuelle Einstellungen sind nur notwendig, wenn Sie zusätzliche Funktionen von smpppd, z. B. die Fernsteuerung, einrichten möchten.

Die Konfigurationsdatei von smpppd ist `/etc/smpppd.conf`. Sie ist so eingestellt, dass standardmäßig keine Fernsteuerung möglich ist. Die wichtigsten Optionen dieser Konfigurationsdatei sind:

open-inet-socket = *`yes|no`*
: Wenn smpppd über das Netzwerk gesteuert werden soll, muss diese Option auf `yes` (ja) eingestellt werden. Der Port, auf dem smpppd lauscht, ist `3185`. Wenn dieser Parameter auf `yes` (ja) gesetzt ist, sollten auch die Parameter `bind-address`, `host-range` und `password` entsprechend eingestellt werden.

bind-address = *`IP-Adresse`*
: Wenn ein Host mehrere IP-Adressen hat, können Sie mit dieser Einstellung festlegen, über welche IP-Adresse smpppd Verbindungen akzeptiert. Standard ist die Überwachung an allen Adressen.

host-range = *`Anfangs-IPEnd-IP`*
: Der Parameter `host-range` definiert einen Netzbereich. Hosts, deren IP-Adressen innerhalb dieses Bereichs liegen, wird der Zugriff auf smpppd gewährt. Alle Hosts, die außerhalb dieses Bereichs liegen, werden abgewiesen.

password = *`Passwort`*
: Mit der Vergabe eines Passworts wird der Client-Zugriff auf autorisierte Hosts beschränkt. Da es lediglich ein reines Textpasswort ist, sollte die Sicherheit, die es bietet, nicht überbewertet werden. Wenn kein Passwort vergeben wird, sind alle Clients berechtigt, auf smpppd zuzugreifen.

slp-register = *`yes|no`*
: Mit diesem Parameter kann der smpppd-Dienst per SLP im Netzwerk bekannt gegeben werden.

Weitere Informationen zu smpppd finden Sie in den man-Seiten zu `smpppd(8)` und `smpppd.conf(5)`.

17.7.2 Konfigurieren von KInternet und cinternet für die Fernsteuerung

KInternet und cinternet können zur Steuerung eines lokalen smpppd verwendet werden. cinternet mit Kommandozeilen ist das Gegenstück zum grafischen KInternet Wenn Sie

diese Dienstprogramme zum Einsatz mit einem entfernten smpppd-Dienst vorbereiten möchten, bearbeiten Sie die Konfigurationsdatei `/etc/smpppd-c.conf` manuell oder mithilfe von KInternet. Diese Datei enthält nur vier Optionen:

sites = *`Liste der Sites`*
: Hier weisen Sie die Frontends an, wo sie nach smpppd suchen sollen. Die Frontends testen die Optionen in der hier angegebenen Reihenfolge. Die Option `Lokal` verlangt den Verbindungsaufbau zum lokalen smpppd. Die Option `Gateway` verweist auf ein smpppd am Gateway. Die Option `config-file` gibt an, dass die Verbindung zum smpppd hergestellt werden sollte, der in den Optionen `Server` und `Port` in der Datei `/etc/smpppd-c.conf` angegeben ist. `slp` veranlasst, dass die Front-Ends eine Verbindung zu einem über SLP gefundenen smpppd aufbauen.

server = *`Server`*
: Geben Sie hier den Host an, auf dem smpppd läuft.

port = *`Port`*
: Geben Sie hier den Host an, auf dem smpppd ausgeführt wird.

password = *`Passwort`*
: Geben Sie das Passwort für smpppd ein.

Wenn smpppd aktiv ist, können Sie jetzt versuchen, darauf zuzugreifen, z. B. mit dem Befehl `cinternet--verbose --interface-list`. Sollten Sie an dieser Stelle Schwierigkeiten haben, finden Sie weitere Informationen in den man-Seiten zu `smpppd-c.conf(5)` und `cinternet(8)`.

18 Drahtlose Kommunikation

Über Wireless LAN kann die Kommunikation zwischen Computern mit SUSE® Linux Enterprise Server hergestellt werden. In diesem Kapitel werden die Konzepte sowie die grundlegende Konfiguration des drahtlosen Networking vorgestellt.

18.1 Wireless LAN

Wireless LANs sind zu einem unverzichtbaren Aspekt der mobilen Computernutzung geworden. Heutzutage verfügen die meisten Notebooks über eingebaute WLAN-Karten. Standard 802.11 für die drahtlose Kommunikation mit WLAN-Karten wurde von der Organisation IEEE erarbeitet. Ursprünglich sah dieser Standard eine maximale Übertragungsrate von 2 MBit/s vor. Inzwischen wurden jedoch mehrere Ergänzungen hinzugefügt, um die Datenrate zu erhöhen. Diese Ergänzungen definieren Details wie Modulation, Übertragungsleistung und Übertragungsraten (siehe Tabelle 18.1, „Überblick über verschiedene WLAN-Standards“ (S. 287)). Zusätzlich implementieren viele Firmen Hardware mit herstellerspezifischen Funktionen oder Funktionsentwürfen.

Tabelle 18.1 *Überblick über verschiedene WLAN-Standards*

Name	Band (GHz)	Maximale Übertragungsrate (MBit/s)	Hinweis
802.11 Vorläufer	2.4	2	Veraltet; praktisch keine Endgeräte verfügbar

Name	Band (GHz)	Maximale Übertragungsrate (MBit/s)	Hinweis
802.11a	5	54	Weniger anfällig für Interferenzen
802.11b	2.4	11	Weniger üblich
802.11g	2.4	54	Weit verbreitet, abwärtskompatibel mit 11b
802.11n-Entwurf	2.4 und/oder 5	300	Common

Ältere 802.11-Karten werden nicht von SUSE® Linux Enterprise Server unterstützt. Die meisten Karten, die 802.11a-, 802.11b-, 802.11g- und 802.11n-Entwurfsversionen verwenden, werden unterstützt. Neuere Karten entsprechen in der Regel dem Standardentwurf 802.11n, Karten, die 802.11g verwenden, sind jedoch noch immer erhältlich.

18.1.1 Funktion

Bei der Arbeit mit drahtlosen Netzwerken werden verschiedene Verfahren und Konfigurationen verwendet, um schnelle, qualitativ hochwertige und sichere Verbindungen herzustellen. Verschiedene Betriebstypen passen zu verschiedenen Einrichtungen. Die Auswahl der richtigen Authentifizierungsmethode kann sich schwierig gestalten. Die verfügbaren Verschlüsselungsmethoden weisen unterschiedliche Vor- und Nachteile auf.

Grundsätzlich lassen sich drahtlose Netzwerke in verwaltete Netzwerke und Ad-hoc-Netzwerke unterteilen. Verwaltete Netzwerke verfügen über ein verwaltendes Element: den Zugriffspunkt In diesem Modus (auch als Infrastrukturmodus bezeichnet) laufen alle Verbindungen der WLAN-Stationen im Netzwerk über den Zugriffspunkt, der auch als Verbindung zu einem Ethernet fungieren kann. Ad-hoc-Netzwerke weisen keinen Zugriffspunkt auf. Die Stationen kommunizieren direkt miteinander, daher ist ein Ad-hoc-Netzwerk in der Regel schneller als ein verwaltetes Netzwerk. Übertragungsbereich und Anzahl der teilnehmenden Stationen sind jedoch in Ad-hoc-Netzwerken stark eingeschränkt. Sie unterstützen auch keine WPA-Authentifizierung. Daher wird gewöhnlich

ein Zugriffspunkt verwendet. Es ist sogar möglich, eine WLAN-Karte als Zugriffspunkt zu verwenden. Einige Karten unterstützen diese Funktionen.

Authentifizierung

Da ein drahtloses Netzwerk wesentlich leichter abgehört und manipuliert werden kann als ein Kabelnetzwerk, beinhalten die verschiedenen Standards Authentifizierungs- und Verschlüsselungsmethoden. In der ursprünglichen Version von Standard IEEE 802.11 werden diese Methoden unter dem Begriff WEP beschrieben. Da sich WEP jedoch als unsicher herausgestellt hat (siehe „Sicherheit“ (S. 296)), hat die WLAN-Branche (gemeinsam unter dem Namen *Wi-Fi Alliance*) die neue Erweiterung WPA definiert, bei dem die Schwächen von WEP ausgemerzt sein sollen. Der spätere Standard IEEE 802.11i (auch als WPA2 bezeichnet, da WPA auf einer Entwurfsfassung von 802.11i beruht) beinhaltet WPA sowie einige andere Authentifizierungs- und Verschlüsselungsmethoden.

Um sicherzugehen, dass nur authentifizierte Stationen eine Verbindung herstellen können, werden in verwalteten Netzwerken verschiedene Authentifizierungsmechanismen verwendet.

Geöffnet
: Ein offenes System ist ein System, bei dem keinerlei Authentifizierung erforderlich ist. Jede Station kann dem Netzwerk beitreten. Dennoch kann WEP-Verschlüsselung (siehe „Verschlüsselung“ (S. 291)) verwendet werden.

Gemeinsamer Schlüssel (gemäß IEEE 802.11)
: In diesem Verfahren wird der WEP-Schlüssel zur Authentifizierung verwendet. Dieses Verfahren wird jedoch nicht empfohlen, da es den WEP-Schlüssel anfälliger für Angriffe macht. Angreifer müssen lediglich lang genug die Kommunikation zwischen Station und Zugriffspunkt abhören. Während des Authentifizierungsvorgangs tauschen beide Seiten dieselben Informationen aus, einmal in verschlüsselter, und einmal in unverschlüsselter Form. Dadurch kann der Schlüssel mit den geeigneten Werkzeugen rekonstruiert werden. Da bei dieser Methode der WEP-Schlüssel für Authentifizierung udn Verschlüsselung verwendet wird, wird die Sicherheit des Netzwerks nicht erhöht. Eine Station, die über den richtigen WEP-Schlüssel verfügt, kann Authentifizierung, Verschlüsselung und Entschlüsselung durchführen. Eine Station, die den Schlüssel nicht besitzt, kann keine empfangenden Pakete entschlüsseln. Sie kann also nicht kommunizieren, unabhängig davon, ob sie sich authentifizieren musste.

WPA-PSK (gemäß IEEE 802.1x)
: WPA-PSK (PSK steht für "preshared key") funktioniert ähnlich wie das Verfahren mit gemeinsamen Schlüssel. Alle teilnehmenden Stationen sowie der Zugriffspunkt benötigen denselben Schlüssel. Der Schlüssel ist 256 Bit lang und wird normalerweise als Passwortsatz eingegeben. Dieses System benötigt keine komplexe Schlüsselverwaltung wie WPA-EAP und ist besser für den privaten Gebrauch geeignet. Daher wird WPA-PSK zuweilen als WPA "Home" bezeichnet.

WPA-EAP (gemäß IEEE 802.1x)
: Eigentlich ist WPA-EAP kein Authentifizierungssystem, sondern ein Protokoll für den Transport von Authentifizierungsinformationen. WPA-EAP dient zum Schutz drahtloser Netzwerke in Unternehmen. Bei privaten Netzwerken wird es kaum verwendet. Aus diesem Grund wird WPA-EAP zuweilen als WPA "Enterprise" bezeichnet.

  WPA-EAP benötigt einen Radius-Server zur Authentifizierung von Benutzern. EAP bietet drei verschiedene Methoden zum Verbinden und Authentifizieren des Servers: TLS (Transport Layer Security), TTLS (Tunneled Transport Layer Security) und PEAP (Protected Extensible Authentication Protocol). Kurz gesagt, funktionieren diese Optionen wie folgt:

  EAP-TLS
  : TLS-Authentifizierung beruht auf dem gegenseitigen Austausch von Zertifikaten für Server und Client. Zuerst legt der Server sein Zertifikat dem Client vor, der es auswertet. Wenn das Zertifikat als gültig betrachtet wird, legt im Gegenzug der Client sein eigenes Zertifikat dem Server vor. TLS ist zwar sicher, erfordert jedoch eine funktionierende Infrastruktur zur Zertifikatsverwaltung im Netzwerk. Diese Infrastruktur ist in privaten Netzwerken selten gegeben.

  EAP-TTLS und PEAP
  : TTLS und PEAP sind zweistufige Protokolle. In der ersten Stufe wird eine sichere Verbindung hergestellt und in der zweiten werden die Daten zur Client-Authentifizierung ausgetauscht. Sie erfordern einen wesentlich geringeren Zertifikatsverwaltungs-Overhead als TLS, wenn überhaupt.

Verschlüsselung

Es gibt verschiedene Verschlüsselungsmethoden, mit denen sichergestellt werden soll, dass keine nicht autorisierten Personen die in einem drahtlosen Netzwerk ausgetauschten Datenpakete lesen oder Zugriff auf das Netzwerk erlangen können:

WEP (in IEEE 802.11 definiert)
: Dieser Standard nutzt den Verschlüsselungsalgorithmus RC4, der ursprünglich eine Schlüssellänge von 40 Bit aufwies, später waren auch 104 Bit möglich. Die Länge wird häufig auch als 64 Bit bzw. 128 Bit angegeben, je nachdem, ob die 24 Bit des Initialisierungsvektors mitgezählt werden. Dieser Standard weist jedoch eigene Schwächen auf. Angriffe gegen von diesem System erstellte Schlüssel können erfolgreich sein. Nichtsdestoweniger ist es besser, WEP zu verwenden, als das Netzwerk überhaupt nicht zu verschlüsseln.

  Einige Hersteller haben "Dynamic WEP" implementiert, das nicht dem Standard entspricht. Es funktioniert exakt wie WEP und weist dieselben Schwächen auf, außer der Tatsache, dass der Schlüssel regelmäßig von einem Schlüsselverwaltungsdienst geändert wird.

TKIP (in WPA/IEEE 802.11i definiert)
: Dieses im WPA-Standard definierte Schlüsselverwaltungsprotokoll verwendet denselben Verschlüsselungsalgorithmus wie WEP, weist jedoch nicht dessen Schwächen auf. Da für jedes Datenpaket ein neuer Schlüssel erstellt wird, sind Angriffe gegen diese Schlüssel vergebens. TKIP wird in Verbindung mit WPA-PSK eingesetzt.

CCMP (in IEEE 802.11i definiert)
: CCMP beschreibt die Schlüsselverwaltung. Normalerweise wird sie in Verbindung mit WPA-EAP verwendet, sie kann jedoch auch mit WPA-PSK eingesetzt werden. Die Verschlüsselung erfolgt gemäß AES und ist stärker als die RC4-Verschlüsselung des WEP-Standards.

18.1.2 Konfiguration mit YaST

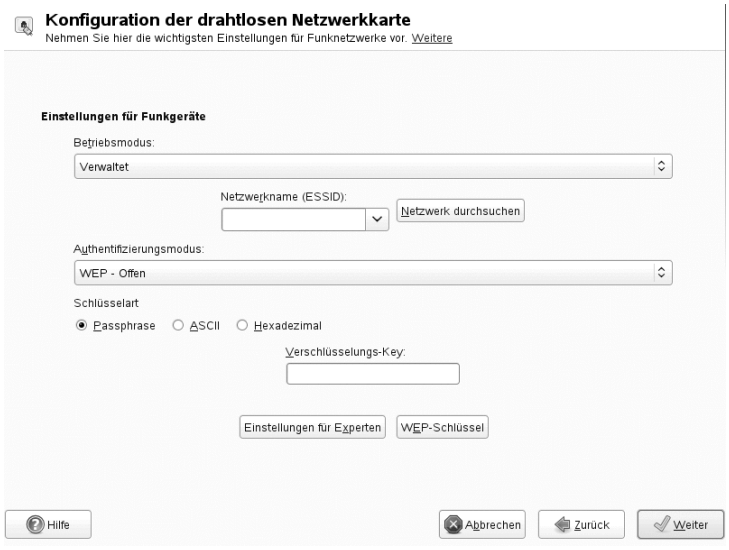
Zum Konfigurieren der drahtlosen Netzwerkkarte wählen Sie im YaST-Kontrollzentrum die Optionen *Netzwerkgeräte* > *Netzwerkeinstellungen* aus. Das Dialogfeld "Netzwerkeinstellungen" wird geöffnet, in dem Sie allgemeine Netzwerkeinstellungen konfigurieren können. Weitere Informationen zur Netzwerkkonfiguration allgemein finden Sie unter

Abschnitt 17.4, „Konfigurieren von Netzwerkverbindungen mit YaST“ (S. 240). Alle vom System erkannten Netzwerkkarten werden auf dem Karteireiter *Übersicht* aufgelistet.

Wählen Sie die drahtlose Karte aus der Liste aus und klicken Sie auf *Bearbeiten*, um das Dialogfeld "Einrichten von Netzwerkkarten" zu öffnen. Nehmen Sie auf dem Karteireiter *Adresse* die Konfiguration zur Verwendung einer dynamischen oder einer statischen IP-Adresse vor. Sie können auch die Einstellungen unter *Allgemein* und *Hardware* wie zum Beispiel *Geräte-Aktivierung* oder *Firewall-Zone* sowie die Treibereinstellungen anpassen. In den meisten Fällen ist es nicht erforderlich, die vorkonfigurierten Werte zu ändern.

Klicken Sie auf *Weiter*, um mit der Konfiguration der drahtlosen Netzwerkkarten im dafür vorgesehenen Dialogfeld fortzufahren. Wenn Sie NetworkManager verwenden (weitere Informationen dazu finden Sie unterAbschnitt 17.5, „NetworkManager“ (S. 266)), ist es nicht erforderlich, die Einstellungen für drahtlose Gerät anzupassen, da diese von NetworkManager nach Bedarf festgelegt werden – fahren Sie mit *Weiter* und *Ja* fort, um die Konfiguration fertig zu stellen. Wenn Sie Ihren Computer nur in einem speziellen drahtlosen Netzwerk verwenden, nehmen Sie hier die grundlegenden Einstellungen für den WLAN-Betrieb vor.

Abbildung 18.1 *YaST: Konfigurieren der WLAN-Karte*



Betriebsmodus
: Eine Station kann in drei verschiedenen Modi in ein WLAN integriert werden. Der geeignete Modus hängt vom Netzwerk ab, in dem kommuniziert werden soll: *Ad-hoc* (Peer-to-Peer-Netzwerk ohne Zugriffspunkt), *Verwaltet* (Netzwerk wird über Zugriffspunkt verwaltet) oder *Master* (Ihre Netzwerkkarte soll als Zugriffspunkt verwendet werden). Um einen der WPA-PSK- oder WPA-EAP-Modi zu verwenden, muss der Betriebsmodus auf *Verwaltet* gesetzt sein.

Netzwerkname (ESSID)
: Alle Stationen in einem drahtlosen Netzwerk benötigen dieselbe ESSID zur Kommunikation untereinander. Wenn nichts angegeben ist, kann die Karte automatisch einen Zugriffspunkt auswählen, der möglicherweise von dem von Ihnen vorgesehenen abweicht. Verwenden Sie *Scan Network* (Netzwerk-Scan), um eine Liste der verfügbaren Netzwerke zu erhalten.

Authentifizierungsmodus
: Wählen Sie eine passende Authentifizierungsmethode für Ihr Netzwerk aus: *Keine Verschlüsselung*, *WEP-Open*, *WEP-Shared Key*, *WPA-EAP* oder *WPA-PSK*. Bei Auswahl der WPA-Authentifizierung muss ein Netzwerkname (ESSID) festgelegt werden.

Art der Schlüsseleingabe
: Die WEP- und WPA-PSK-Authentifizierung verlangt die Eingabe eines Schlüssels. Der Schlüssel muss entweder als *Passwortsatz*, als *ASCII*-String oder als*Hexadezimal*-String eingegeben werden.

  WEP-Schlüssel
  : Geben Sie hier entweder den Standardschlüssel ein oder klicken Sie auf *WEP-Schlüssel*, um das erweiterte Dialogfeld für die Schlüsselkonfiguration zu öffnen. Legen Sie die Länge des Schlüssels auf *128 Bit* oder *64 Bit* fest. Die Standardeinstellung ist *128 Bit*. Im Listenbereich unten im Dialogfeld können bis zu vier verschiedene Schlüssel angegeben werden, die Ihre Station für die Verschlüsselung verwenden soll. Wählen Sie *Als Standard festlegen*, um einen davon als Standardschlüssel festzulegen. Wenn Sie hier keine Auswahl treffen, verwendet YaST den als erstes eingegebenen Schlüssel als Standardschlüssel. Wenn der Standardschlüssel gelöscht wird, muss einer der anderen Schlüssel manuell als Standardschlüssel gekennzeichnet werden. Klicken Sie auf *Bearbeiten*, um bestehende Listeneinträge zu bearbeiten oder neue Schlüssel zu erstellen. In diesem Fall werden Sie über ein Popup-Fenster dazu aufgefordert, einen Eingabetyp auszuwählen (*Passwortsatz*, *ASCII* oder *Hexadezimal*). Geben

Sie bei Verwendung von *Passwortsatz* ein Wort oder eine Zeichenkette ein, aus der ein Schlüssel mit der zuvor festgelegten Länge erstellt wird. *ASCII* erfordert die Eingabe von 5 Zeichen für einen 64-Bit-Schlüssel und von 13 Zeichen für einen 128-Bit-Schlüssel. Bei *Hexadezimal* geben Sie 10 Zeichen für einen 64-Bit-Schlüssel bzw. 26 Zeichen für einen 128-Bit-Schlüssel in Hexadezimalnotation ein.

WPA-PSK
: Um einen Schlüssel für WPA-PSK einzugeben, stehen die Eingabemethoden *Passwortsatz* bzw. *Hexadezimal* zur Auswahl. Im Modus *Passwortsatz* muss die Eingabe 8 bis 63 Zeichen betragen. Im Modus *Hexadezimal* geben Sie 64 Zeichen ein.

Einstellungen für Experten
: Mit dieser Schaltfläche wird ein Dialogfeld für die detaillierte Konfiguration der WLAN-Verbindung geöffnet. Normalerweise sollte es nicht erforderlich sein, die vorkonfigurierten Einstellungen zu ändern.

Channel
: Die Spezifikation eines Kanals, über den die WLAN-Station arbeiten soll, ist nur in den Modi *Ad-hoc* und *Master* erforderlich. Im Modus *Verwaltet* durchsucht die Karte automatisch die verfügbaren Kanäle nach Zugriffspunkten. Im Modus *Ad-hoc* müssen Sie einen der angebotenen Kanäle (11 bis 14, abhängig von Ihrem Land) für die Kommunikation zwischen Ihrer Station und den anderen Stationen auswählen. Im Modus *Master* müssen Sie festlegen, auf welchem Kanal Ihre Karte die Funktionen des Zugriffspunkts anbieten soll. Die Standardeinstellung für diese Option lautet *Auto*.

Bitrate
: Je nach der Leistungsfähigkeit Ihres Netzwerks können Sie eine bestimmte Bitrate für die Übertragung von einem Punkt zum anderen festlegen. Bei der Standardeinstellung, *Auto*, versucht das System, die höchstmögliche Datenübertragungsrate zu verwenden. Einige WLAN-Karten unterstützen die Festlegung von Bitraten nicht.

Zugriffspunkt
: In einer Umgebung mit mehreren Zugriffspunkten kann einer davon durch Angabe der MAC-Adresse vorausgewählt werden.

Energieverwaltung verwenden

Wenn Sie Ihr Notebook unterwegs verwenden, sollten Sie die Akku-Betriebsdauer mithilfe von Energiespartechnologien maximieren. Weitere Informationen über die Energieverwaltung finden Sie in Kapitel 15, *Energieverwaltung* (S. 193). Die Verwendung der Energieverwaltung kann die Verbindungsqualität beeinflussen und die Netzwerklatenz erhöhen.

Klicken Sie auf "Weiter", um die Einrichtung fertig zu stellen. Wenn Sie die WPA-EAP-Authentifizierung gewählt haben, ist ein weiterer Konfigurationsschritt erforderlich, bevor Ihr Arbeitsplatzrechner im WLAN bereitgestellt werden kann. Geben Sie den Berechtigungsnachweis ein, den Sie von Ihrem Netzwerkadministrator erhalten haben. Geben Sie für TLS *Identität*, *Client-Zertifikat*, *Client-Schlüssel* und *Server-Zertifikat* an. Für TTLS und PEAP sind *Identität* und *Passwort* erforderlich. Die Optionen *Server-Zertifikat* und *Anonyme Identität* sind optional. YaST sucht unter `/etc/cert` nach einem Zertifikat. Speichern Sie daher die erhaltenen Zertifikate an diesem Ort und schränken Sie den Zugriff zu diesen Dateien auf `0600` (Lese- und Schreibzugriff des Eigentümers) ein. Klicken Sie auf *Details*, um das Dialogfeld für die erweiterte Authentifizierung für die WPA-EAP-Einrichtung aufzurufen. Wählen Sie die Authentifizierungsmethode für die zweite Phase der EAP-TTLS- oder EAP-PEAP-Kommunikation aus. Wenn Sie im vorherigen Dialogfeld TTLS ausgewählt haben, wählen Sie `any`, `MD5`, `GTC`, `CHAP`, `PAP`, `MSCHAPv1` oder `MSCHAPv2`. Wenn Sie PEAP ausgewählt haben, wählen Sie `any`, `MD5`, `GTC` oder `MSCHAPv2`. *PEAP-Version* kann verwendet werden, um die Verwendung einer bestimmten PEAP-Implementierung zu erzwingen, falls die automatisch festgelegte Einstellung für Sie nicht funktioniert.

WICHTIG: Sicherheit in drahtlosen Netzwerken.

Sie sollten unbedingt eine der unterstützten Authentifizierungs- und Verschlüsselungsmethoden für den Schutz Ihres Netzwerks verwenden. Bei nicht verschlüsselten WLAN-Verbindungen können Dritte alle Netzwerkdaten abfangen. Selbst eine schwache Verschlüsselung (WEP) ist besser als gar keine. Weitere Informationen hierzu erhalten Sie in „Verschlüsselung“ (S. 291) und „Sicherheit“ (S. 296).

18.1.3 Dienstprogramme

Das Paket `wireless-tools` enthält Dienstprogramme, mit denen Sie Wireless-LAN-spezifische Parameter festlegen und Statistiken abrufen können. Weitere Informa-

tionen finden Sie unter `http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.html`.

18.1.4 Tipps und Tricks zur Einrichtung eines WLAN

Mit diesen Tipps können Sie Geschwindigkeit und Stabilität sowie Sicherheitsaspekte Ihres WLAN optimieren.

Stabilität und Geschwindigkeit

Leistungsfähigkeit und Zuverlässigkeit eines drahtlosen Netzwerks hängen in erster Linie davon ab, ob die teilnehmenden Stationen ein sauberes Signal von den anderen Stationen empfangen. Hindernisse, wie beispielsweise Wände, schwächen das Signal erheblich ab. Je weiter die Signalstärke sinkt, desto langsamer wird die Übertragung. Während des Betriebs können Sie die Signalstärke mit dem Dienstprogramm iwconfig in der Kommandozeile (Feld `Link-Qualität`) oder mit NetworkManager oder KNetworkManager überprüfen. Bei Problemen mit der Signalqualität sollten Sie versuchen, die Geräte an einer anderen Position einzurichten oder die Antennen der Zugriffspunkte neu zu positionieren. Hilfsantennen, die den Empfang erheblich verbessern sind für eine Reihe von PCMCIA-WLAN-Karten erhältlich. Die vom Hersteller angegebene Rate, beispielsweise 54 MBit/s, ist ein Nennwert, der für das theoretische Maximum steht. IN der Praxis beträgt der maximale Datendurchsatz nicht mehr als die Hälfte dieses Werts.

Sicherheit

Wenn Sie ein drahtloses Netzwerk einrichten möchten, sollten Sie bedenken, dass jeder, der sich innerhalb der Übertragungsreichweite befindet, problemlos auf das Netzwerk zugreifen kann, sofern keine Sicherheitsmaßnahmen implementiert sind. Daher sollten Sie auf jeden Fall eine Verschlüsselungsmethode aktivieren. Alle WLAN-Karten und Zugriffspunkte unterstützen WEP-Verschlüsselung. Dieses Verfahren bietet zwar keine absolute Sicherheit, es stellt jedoch durchaus ein Hindernis für mögliche Angreifer dar. WEP ist für den privaten Gebrauch in der Regel ausreichend. WPA-PSK bietet noch größere Sicherheit, es ist jedoch in älteren Zugriffspunkten und Routern mit WLAN-Funktionen nicht implementiert. Auf einigen Geräten kann WPA mithilfe einer Firmware-Aktualisierung implementiert werden. Zudem unterstützt Linux zwar WPA auf

den meisten Hardwarekomponenten, jedoch bieten einige Treiber keine WPA-Unterstützung. Wenn WPA nicht verfügbar ist, sollten Sie lieber WEP verwenden, als völlig auf Verschlüsselung zu verzichten. Bei Unternehmen mit erhöhten Sicherheitsanforderungen sollten drahtlose Netzwerke ausschließlich mit WPA betrieben werden.

18.1.5 Fehlersuche

Wenn Ihre WLAN-Karte nicht reagiert, überprüfen Sie, ob Sie die benötigte Firmware heruntergeladen haben. Weitere Informationen finden Sie in `/usr/share/doc/packages/wireless-tools/README.firmware`.

Mehrere Netzwerkgeräte

Moderne Laptops verfügen normalerweise über eine Netzwerkkarte und eine WLAN-Karte. Wenn Sie beide Geräte mit DHCP (automatische Adresszuweisung) konfiguriert haben, können Probleme mit der Namenauflösung und dem Standard-Gateway auftreten. Dies können Sie daran erkennen, dass Sie dem Router ein Ping-Signal senden, jedoch nicht das Internet verwenden können. In der Support-Datenbank finden Sie unter `http://en.opensuse.org/SDB:Name_Resolution_Does_Not_Work_with_Several_Concurrent_DHCP_Clients` einen Artikel zu diesem Thema.

Probleme mit Prism2-Karten

Für Geräte mit Prism2-Chips sind mehrere Treiber verfügbar. Die verschiedenen Karten funktionieren mit den einzelnen Treibern mehr oder weniger reibungslos. Bei diesen Karten ist WPA nur mit dem hostap-Treiber möglich. Wenn eine solche Karte nicht einwandfrei oder überhaupt nicht funktioniert oder Sie WPA verwenden möchten, lesen Sie nach unter `/usr/share/doc/packages/wireless-tools/README.prism2`.

18.1.6 Weiterführende Informationen

Auf den Internetseiten von Jean Tourrilhes, dem Entwickler der *Wireless Tools* für Linux finden Sie ein breites Spektrum an nützlichen Informationen zu drahtlosen Netzwerken. Weitere Informationen hierzu finden Sie unter `http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Wireless.html`.

19 SLP-Dienste im Netzwerk

Das *Service Location Protocol* (SLP) wurde entwickelt, um die Konfiguration vernetzter Clients innerhalb eines lokalen Netzwerks zu vereinfachen. Zur Konfiguration eines Netzwerk-Clients inklusive aller erforderlichen Dienste benötigt der Administrator traditionell detailliertes Wissen über die im Netzwerk verfügbaren Server. SLP teilt allen Clients im lokalen Netzwerk die Verfügbarkeit ausgewählter Dienste mit. Anwendungen mit SLP-Unterstützung können diese Informationen verarbeiten und können automatisch konfiguriert werden.

SUSE® Linux Enterprise Server unterstützt die Installation von mit SLP bereitgestellten Installationsquellen und beinhaltet viele Systemdienste mit integrierter Unterstützung für SLP. YaST und Konqueror verfügen beide über SLP-fähige Frontends. Nutzen Sie SLP, um vernetzten Clients zentrale Funktionen wie Installationsserver, YOU-Server, Dateiserver oder Druckserver auf Ihrem System zur Verfügung zu stellen.

WICHTIG: SLP-Unterstützung in SUSE Linux Enterprise Server

Dienste, die SLP-Unterstützung bieten, sind u. a. cupsd, rsyncd, ypserv, openldap2, ksysguardd, saned, kdm, vnc, login, smpppd, rpasswd, postfix und sshd (über fish).

19.1 Installation

Nur ein SLP-Client und slptools werden standardmäßig installiert. Wenn Sie Dienste über SLP bereitstellen möchten, installieren Sie das Paket `openslp-server`. Zur Installation des Pakets starten Sie YaST und wählen Sie *Software* > *Software-Manage-*

ment aus. Wählen Sie dann *Filter* > *Schemata* und klicken Sie auf *Verschiedene Server*. Wählen Sie `openslp-server`. Bestätigen Sie die Installation der erforderlichen Pakete, um den Installationsvorgang abzuschließen.

19.2 SLP aktivieren

slpd muss auf Ihrem System ausgeführt werden, damit Dienste mit SLP angeboten werden können. Wenn der Computer nur als Client fungieren soll und keine Dienste anbietet, ist es nicht erforderlich, slpd auszuführen. Wie die meisten Systemdienste unter SUSE Linux Enterprise Server wird der slpd-Daemon über ein separates `init`-Skript gesteuert. Nach der Installation ist der Daemon standardmäßig inaktiv. Wenn Sie ihn temporär aktivieren möchten, führen Sie `rcslpd start` als `root` aus. Zum Stoppen führen Sie `rcslpd stop` aus. Mit `restart` oder `status` lösen Sie einen Neustart oder eine Statusabfrage aus. Wenn slpd nach dem Booten immer aktiv sein soll, aktivieren Sie slpd in YaST *System* > *Systemdienste (Runlevel)* oder führen Sie das Kommando `insserv slpd` als `root` aus. Dies beinhaltet slpd in der Gruppe von Diensten, die beim Booten gestartet werden.

19.3 SLP-Frontends in SUSE Linux Enterprise Server

Verwenden Sie ein SLP-Frontend, um in Ihrem Netzwerk von SLP bereitgestellte Dienste zu finden. SUSE Linux Enterprise Server enthält mehrere Frontends:

slptool
: slptool ist ein einfaches Kommandozeilenprogramm, mit dem proprietäre Dienste oder SLP-Anfragen im Netzwerk bekannt gegeben werden können. Mit `slptool --help` werden alle verfügbaren Optionen und Funktionen aufgelistet. slptool kann auch aus Skripten aufgerufen werden, die SLP-Informationen verarbeiten. Um beispielsweise alle Netzwerk-Zeitserver zu finden, die sich selbst im aktuellen Netzwerk ankündigen, führen Sie folgendes Kommando aus:

  ```
  slptool findsrvs service:ntp
  ```

YaST
: In YaST steht auch ein SLP-Browser zur Verfügung. Jedoch ist dieser Browser nicht über das YaST-Kontrollzentrum zugreifbar. Führen Sie zum Starten dieses YaST-Moduls `yast2 slp` als `root`-Benutzer aus. Klicken Sie auf die unterschiedlichen Protokolle am linken Rand der Benutzerschnittstelle, um weitere Informationen über den betreffenden Dienst zu erhalten.

19.4 Installation über SLP

Wenn Sie einen Installationsserver mit SUSE Linux Enterprise Server-Installationsmedien in Ihrem Netzwerk anbieten, kann dieser mit SLP registriert werden. Weitere Informationen finden Sie in Abschnitt „Einrichten des Servers, auf dem sich die Installationsquellen befinden“ (Kapitel 14, *Installation mit entferntem Zugriff*, ↑*Bereitstellungshandbuch*). Wenn die SLP-Installation ausgewählt wurde, startet linuxrc eine SLP-Anrage, nachdem das System vom ausgewählten Startmedium gestartet wurde, und zeigt die gefundenen Quellen an.

19.5 Bereitstellen von Diensten über SLP

Viele Anwendungen in SUSE Linux Enterprise Server verfügen durch die `libslp`-Bibliothek über eine integrierte SLP-Unterstützung. Falls ein Dienst ohne SLP-Unterstützung kompiliert wurde, können Sie ihn mit einer der folgenden Methoden per SLP verfügbar machen:

Statische Registrierung über `/etc/slp.reg.d`
: Legen Sie für jeden neuen Dienst eine separate Registrierungsdatei an. Dies ist ein Beispiel einer solchen Datei für die Registrierung eines Scannerdiensts:

```
## Register a saned service on this system
## en means english language
## 65535 disables the timeout, so the service registration does
## not need refreshes
service:scanner.sane://$HOSTNAME:6566,en,65535
watch-port-tcp=6566
description=SANE scanner daemon
```

Die wichtigste Zeile dieser Datei ist die *Dienst-URL*, die mit `service:` beginnt. Sie enthält den Diensttyp (`scanner.sane`) und die Adresse, unter der der Dienst auf dem Server verfügbar ist. *`$HOSTNAME`* wird automatisch durch den vollständigen Hostnamen ersetzt. Abgetrennt durch einen Doppelpunkt folgt nun der Name des TCP-Ports, auf dem der entsprechende Dienst gefunden werden kann. Geben Sie nun die Sprache an, in der der Dienst angekündigt werden soll, und die Gültigkeitsdauer der Registrierung in Sekunden. Diese Angaben müssen durch Kommas von der Dienst-URL getrennt werden. Wählen Sie für die Registrierungsdauer einen Wert zwischen `0` und `65535`. `0` verhindert die Registrierung. Mit `65535` werden alle Einschränkungen aufgehoben.

Die Registrierungsdatei enthält außerdem die beiden Variablen `watch-port-tcp` und `description`. `watch-port-tcp` koppelt die SLP-Dienstankündigung daran, ob der entsprechende Dienst aktiv ist, indem slpd den Status des Diensts überprüft. Die zweite Variable enthält eine genauere Beschreibung des Diensts, die in den entsprechenden Browsern angezeigt wird.

TIPP: YaST und SLP

Einige von YaST bereitgestellte Dienste, wie ein Installationsserver oder YOU-Server, führen diese Registrierung automatisch aus, wenn Sie SLP in den Modul-Dialogfeldern aktivieren. YaST erstellt dann Registrierungsdateien für diese Dienste.

Statische Registrierung über `/etc/slp.reg`
: Der einzige Unterschied zwischen dieser Methode und der Prozedur mit `/etc/slp.reg.d` besteht darin, dass alle Dienste in einer zentralen Datei gruppiert sind.

Dynamische Registrierung über slptool
: Wenn ein Dienst dynamisch ohne Verwendung von Konfigurationsdateien registriert werden soll, verwenden Sie das Kommandozeilenprogramm slptool. Dasselbe Programm kann auch die Registrierung eines bestehenden Dienstangebots aufheben, ohne slpd neu zu starten.

19.6 Weiterführende Informationen

Weitere Informationen zu SLP finden Sie in folgenden Quellen:

RFC 2608, 2609, 2610
: RFC 2608 befasst sich mit der Definition von SLP im Allgemeinen. RFC 2609 geht näher auf die Syntax der verwendeten Dienst-URLs ein und RFC 2610 thematisiert DHCP über SLP.

`http://www.openslp.org/`
: Die Homepage des OpenSLP-Projekts.

`/usr/share/doc/packages/openslp`
: Dieses Verzeichnis enthält alle verfügbaren Dokumentationen zu SLP, einschließlich einer `README.SuSE`-Datei mit Details zu SUSE Linux Enterprise Server, der oben genannten RFCs und zweier einleitender HTML-Dokumente. Programmierer, die an den SLP-Funktionen interessiert sind, finden weitere Informationen im *Programmierhandbuch*, das im Paket `openslp-devel` enthalten ist.

20 Zeitsynchronisierung mit NTP

Der NTP-(Network Time Protocol-)Mechanismus ist ein Protokoll für die Synchronisierung der Systemzeit über das Netzwerk. Erstens kann ein Computer die Zeit von einem Server abrufen, der als zuverlässige Zeitquelle gilt. Zweitens kann ein Computer selbst für andere Computer im Netzwerk als Zeitquelle fungieren. Zwei Ziele sollen erreicht werden: die absolute Zeit beizubehalten und die Systemzeit aller Computer im Netzwerk zu synchronisieren.

Das Aufrechterhalten der genauen Systemzeit ist in vielen Situationen wichtig. Die integrierte Hardware-Uhr (BIOS-Uhr) erfüllt häufig nicht die Anforderungen bestimmter Anwendungen, beispielsweise Datenbanken. Die manuelle Korrektur der Systemzeit würde schwerwiegende Probleme nach sich ziehen; das Zurückstellen kann beispielsweise zu Fehlfunktionen wichtiger Anwendungen führen. Die Systemzeiten der in einem Netzwerk zusammengeschlossenen Computer müssen in der Regel synchronisiert werden. Es empfiehlt sich aber nicht, die Zeiten manuell anzugleichen. Vielmehr sollten Sie dazu ntp verwenden. Er passt die Systemzeit ständig anhand zuverlässiger Zeitserver im Netzwerk an. Zudem ermöglicht er die Verwaltung lokaler Referenzuhren, beispielsweise funkgesteuerter Uhren.

20.1 Konfigurieren eines NTP-Client mit YaST

ntp ist so voreingestellt, dass die lokale Computeruhr als Zeitreferenz verwendet wird. Das Verwenden der (BIOS-) Uhr ist jedoch nur eine Ausweichlösung, wenn keine genauere Zeitquelle verfügbar ist. YaST erleichtert die Konfiguration von NTP-Clients.

Verwenden Sie für Systeme, die keine Firewall ausführen, entweder die schnelle oder die erweiterte Konfiguration. Bei einem durch eine Firewall geschützten System kann die erweiterte Konfiguration die erforderlichen Ports in SuSEfirewall2 öffnen.

20.1.1 Erweiterte NTP-Client-Konfiguration

Sie können den NTP-Client entweder manuell oder automatisch konfigurieren, um eine Liste der NTP-Server zu erhalten, die über DHCP in Ihrem Netzwerk verfügbar sind. Wenn Sie *NTP-Daemon über DHCP konfigurieren* wählen, sind die unten erklärten Optionen nicht verfügbar.

Die Server und anderen Zeitquellen für die Abfrage durch den Client sind im unteren Bereich im Karteireiter *Allgemeine Einstellungen* aufgelistet. Bearbeiten Sie diese Liste nach Bedarf mithilfe der Optionen *Hinzufügen*, *Bearbeiten* und *Löschen*. Mit Protokoll anzeigen können die Protokolldateien Ihres Clients angezeigt werden.

Klicken Sie auf *Hinzufügen*, um eine neue Quelle für Zeitinformationen hinzuzufügen. Wählen Sie im nachfolgenden Dialogfeld den Quellentyp aus, mit dem die Zeitsynchronisierung vorgenommen werden soll. Mit den zur Verfügung stehenden Optionen können Sie:

Server
: Ein weiteres Dialogfeld ermöglicht Ihnen, einen NTP-Server auszuwählen. Aktivieren Sie *Für initiale Synchronisierung verwenden*, um die Synchronisierung der Zeitinformationen zwischen dem Server und dem Client auszulösen, wenn das System gebootet wird. Unter *Optionen* können Sie weitere Optionen für ntpd einstellen.

  Mit den *Access Control Options* (Zugriffskontrolloptionen) können Sie die Aktionen einschränken, die der entfernte Computer mit dem Daemon Ihres Computers ausführen kann. Dieses Feld ist nur aktiviert, wenn die Option *Restrict NTP Service to Configured Servers Only* (NTP-Dienst auf konfigurierte Server beschränken) auf dem Karteireiter *Sicherheitseinstellungen* aktiviert ist. Die Optionen entsprechen den `restrict`-Klauseln der Datei `/etc/ntp.conf`. Die Klausel `nomodify notrap noquery` verhindert beispielsweise, dass der Server die NTP-Einstellungen Ihres Computers ändern und die Trap-Funktion (eine Fernprotokollierungsfunktion für Ereignisse) Ihres NTP-Daemons verwenden kann. Diese Einschränkungen werden besonders für Server außerhalb Ihrer Kontrolle empfohlen (z. B. im Internet).

Ziehen Sie bezüglich detaillierter Informationen `/usr/share/doc/packages/ntp-doc` zurate (Bestandteil des `ntp-doc`-Pakets).

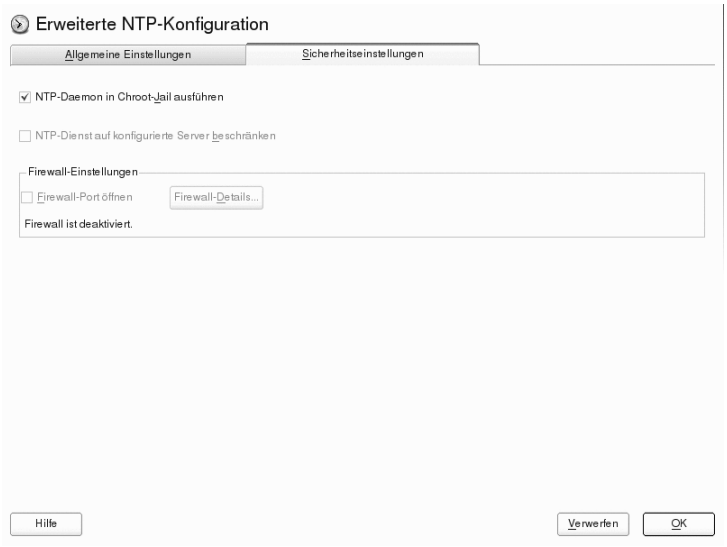
Peer
: Ein Peer ist ein Computer, mit dem eine symmetrische Beziehung eingerichtet wird: Er fungiert sowohl als Zeitserver als auch als Client. Wenn Sie einen Peer im selben Netzwerk anstelle eines Servers verwenden möchten, geben Sie die Adresse des Systems ein. Der Rest des Dialogfelds ist mit dem Dialogfeld *Server* identisch.

Funkuhr
: Wenn eine Funkuhr für die Zeitsynchronisierung in Ihrem System verwendet werden soll, geben Sie Uhrtyp, Gerätezahl, Gerätename und weitere Optionen in diesem Dialogfeld ein. Klicken Sie auf *Treiber-Kalibirierung*, um den Treiber genauer einzustellen. Detaillierte Informationen zum Betrieb einer lokalen Funkuhr finden Sie in `/usr/share/doc/packages/ntp-doc/refclock.html`.

Ausgangs-Broadcast
: Zeitinformationen und Abfragen können im Netzwerk auch per Broadcast übermittelt werden. Geben Sie in diesem Dialogfeld die Adresse ein, an die Broadcasts gesendet werden sollen. Die Option für Broadcasts sollte nur aktiviert werden, wenn Ihnen eine zuverlässige Zeitquelle, etwa eine funkgesteuerte Uhr, zur Verfügung steht.

Eingangs-Broadcast
: Wenn Ihr Client die entsprechenden Informationen per Broadcast erhalten soll, geben Sie in diesen Feldern die Adresse ein, von der die jeweiligen Pakete akzeptiert werden sollen.

Abbildung 20.1 *Erweiterte NTP-Konfiguration: Sicherheitseinstellungen*



Legen Sie auf dem Karteireiter *Sicherheitseinstellungen* fest, ob ntpd in einem "Chroot Jail" gestartet werden soll. Standardmäßig ist *DHCP-Daemon in Chroot-Jail starten* aktiviert. Hierdurch wird die Sicherheit im Falle eines Angriffs über ntpd erhöht, da der Angreifer daran gehindert wird, das gesamte System zu beeinträchtigen.

Die Option *Restrict NTP Service to Configured Servers Only* (NTP-Dienst auf konfigurierte Server beschränken) erhöht die Sicherheit Ihres Systems. Wenn gewählt, verhindert diese Option, dass entfernte Computer die NTP-Einstellungen Ihres Computers anzeigen und ändern und die Trap-Funktion für die Fernprotokollierung von Ereignissen verwenden können. Wenn gewählt, gelten diese Einschränkungen für alle entfernten Computer, es sei denn, Sie überschreiben die Zugriffskontrolloptionen für einzelne Computer in der Liste der Zeitquellen auf dem Karteireiter *Allgemeine Einstellungen*. Allen anderen entfernten Computern wird nur die Abfrage der lokalen Zeit erlaubt.

Aktivieren Sie *Firewall-Port öffnen*, wenn SuSEfirewall2 aktiviert ist (Standardeinstellung). Wenn Sie den Port geschlossen lassen, können Sie keine Verbindung zum Zeitserver herstellen.

20.2 Manuelle Konfiguration von ntp im Netzwerk

Die einfachste Art der Verwendung eines Zeitservers im Netzwerk besteht darin, Serverparameter festzulegen. Beispiel: Wenn der Zeitserver `ntp.example.com` über das Netzwerk erreichbar ist, fügen Sie seinen Namen in die Datei `/etc/ntp.conf` ein, indem Sie folgende Zeile einfügen.

```
server ntp.example.com
```

Wenn Sie weitere Zeitserver hinzufügen möchten, fügen Sie zusätzliche Zeilen mit dem Schlüsselwort `server` ein. Nach der Initialisierung von ntpd mit dem Kommando `rcntpdstart` dauert es etwa eine Stunde, bis die Zeit stabil ist und die Drift-Datei für das Korrigieren der lokalen Computeruhr erstellt wird. Mithilfe der Drift-Datei kann der systematische Fehler der Hardware-Uhr berechnet werden, sobald der Computer eingeschaltet wird. Die Korrektur kommt umgehend zum Einsatz und führt zu einer größeren Stabilität der Systemzeit.

Es gibt zwei Möglichkeiten, den NTP-Mechanismus als Client zu verwenden: Erstens kann der Client in regelmäßigen Abständen die Zeit von einem bekannten Server abfragen. Wenn viele Clients vorhanden sind, kann dies zu einer starken Auslastung des Servers führen. Zweitens kann der Client auf NTP-Broadcasts warten, die von Broadcast-Zeitservern im Netzwerk gesendet werden. Dieser Ansatz hat den Nachteil, dass die Qualität des Servers unbekannt ist und dass ein Server, der falsche Informationen sendet, zu schwerwiegenden Problemen führen kann.

Wenn die Zeit per Broadcast ermittelt wird, ist der Servername nicht erforderlich. Geben Sie in diesem Fall die Zeile `broadcastclient` in die Konfigurationsdatei `/etc/ntp.conf` ein. Wenn ein oder mehrere bekannte Zeitserver exklusiv verwendet werden sollen, geben Sie die Namen in der Zeile ein, die mit `servers` beginnt.

20.3 Einrichten einer lokalen Referenzuhr

Das Software-Paket ntp enthält Treiber für das Verbinden lokaler Referenzuhren. Eine Liste unterstützter Uhren steht im Paket `ntp-doc` in der Datei `/usr/share/doc/`

packages/ntp-doc/refclock.html zur Verfügung. Jeder Treiber ist mit einer Nummer verknüpft. In ntp wird die eigentliche Konfiguration mit Pseudo-IP-Adressen durchgeführt. Die Uhren werden so in die Datei /etc/ntp.conf eingegeben, als ob sie im Netzwerk vorhanden wären. Zu diesem Zweck werden Ihnen spezielle IP-Adressen im Format 127.127.*t*.*u* zugewiesen. Hierbei steht *t* für den Uhrentyp und legt fest, welcher Treiber verwendet wird und *u* steht für die Einheit (unit), die die verwendete Schnittstelle bestimmt.

Im Regelfall verfügen die einzelnen Treiber über spezielle Parameter, die die Konfigurationsdetails beschreiben. Die Datei /usr/share/doc/packages/ntp-doc/drivers/driver*NN*.html (*NN* steht für die Anzahl der Treiber) bietet Informationen zum jeweiligen Uhrentyp. Für die Uhr vom "Typ 8" (Funkuhr über serielle Schnittstelle) ist ein zusätzlicher Modus erforderlich, der die Uhr genauer angibt. Das Conrad DCF77-Empfängermodul weist beispielsweise Modus 5 auf. Wenn diese Uhr als bevorzugte Referenz verwendet werden soll, geben Sie das Schlüsselwort prefer an. Die vollständige server-Zeile für ein Conrad DCF77-Empfängermodul sieht folgendermaßen aus:

```
server 127.127.8.0 mode 5 prefer
```

Für andere Uhren gilt dasselbe Schema. Nach der Installation des Pakets ntp-doc steht die Dokumentation für ntp im Verzeichnis /usr/share/doc/packages/ntp-doc zur Verfügung. Die Datei /usr/share/doc/packages/ntp-doc/refclock.html enthält Links zu den Treiberseiten, auf denen die Treiberparameter beschrieben werden.

20.4 Uhrensynchronisierung mit einer externen Zeitreferenz (ETR)

Unterstützung für Uhrensynchronisierung mit einer externen Zeitreferenz (ETR) ist verfügbar. Die externe Zeitreferenz sendet 2**20 (2 hoch 20) Millisekunden ein Oszillatorsignal und ein Synchronisierungssignal, um die Tageszeit-Uhren aller angeschlossenen Server synchron zu halten.

Zur Verfügbarkeit können zwei ETR-Einheiten an einen Computer angeschlossen werden. Wenn die Uhr um mehr als die Sync-Prüf-Toleranz abweicht, erhalten alle CPUs eine Rechnerprüfung, die darauf hinweist, dass die Uhr nicht synchron ist. In

diesem Fall werden sämtliche DASD-E/A an XRC-fähige Geräte gestoppt, bis die Uhr wieder synchron ist.

Die ETR-Unterstützung wird über zwei `sysfs`-Attribute aktiviert; geben Sie als `root`-Benutzer folgendes ein:

```
echo 1 > /sys/devices/system/etr/etr0/online
echo 1 > /sys/devices/system/etr/etr1/online
```

21 Domain Name System (DNS)

DNS (Domain Name System) ist zur Auflösung der Domänen- und Hostnamen in IP-Adressen erforderlich. Auf diese Weise wird die IP-Adresse 192.168.2.100 beispielsweise dem Hostnamen `jupiter` zugewiesen. Bevor Sie Ihren eigenen Namenserver einrichten, sollten Sie die allgemeinen Informationen zu DNS in Abschnitt 17.3, „Namensauflösung“ (S. 238) lesen. Die folgenden Konfigurationsbeispiele beziehen sich auf BIND.

21.1 DNS-Terminologie

Zone
: Der Domänen-Namespace wird in Regionen, so genannte Zonen, unterteilt. So ist beispielsweise `example.com` der Bereich oder die Zone `example` der Domäne `com`.

DNS-Server
: Der DNS-Server ist ein Server, auf dem der Name und die IP-Informationen für eine Domäne gespeichert sind. Sie können einen primären DNS-Server für die Masterzone, einen sekundären Server für die Slave-Zone oder einen Slave-Server ohne jede Zone für das Caching besitzen.

  DNS-Server der Masterzone
  : Die Masterzone beinhaltet alle Hosts aus Ihrem Netzwerk und der DNS-Server der Masterzone speichert die aktuellen Einträge für alle Hosts in Ihrer Domäne.

DNS-Server der Slave-Zone
: Eine Slave-Zone ist eine Kopie der Masterzone. Der DNS-Server der Slave-Zone erhält seine Zonendaten mithilfe von Zonentransfers von seinem Masterserver. Der DNS-Server der Slave-Zone antwortet autorisiert für die Zone, solange er über gültige (nicht abgelaufene) Zonendaten verfügt. Wenn der Slave keine neue Kopie der Zonendaten erhält, antwortet er nicht mehr für die Zone.

Forwarder
: Forwarders sind DNS-Server, an die der DNS-Server Abfragen sendet, die er nicht bearbeiten kann. Zum Aktivieren verschiedener Konfigurationsquellen in einer Konfiguration wird `netconfig` verwendet (siehe auch `man 8 netconfig`).

Datensatz
: Der Eintrag besteht aus Informationen zu Namen und IP-Adresse. Die unterstützten Einträge und ihre Syntax sind in der BIND-Dokumentation beschrieben. Einige spezielle Einträge sind beispielsweise:

  NS-Eintrag
  : Ein NS-Eintrag informiert die Namenserver darüber, welche Computer für eine bestimmte Domänenzone zuständig sind.

  MX-Eintrag
  : Die MX (Mailaustausch)-Einträge beschreiben die Computer, die für die Weiterleitung von Mail über das Internet kontaktiert werden sollen.

  SOA-Eintrag
  : Der SOA (Start of Authority)-Eintrag ist der erste Eintrag in einer Zonendatei. Der SOA-Eintrag wird bei der Synchronisierung von Daten zwischen mehreren Computern über DNS verwendet.

21.2 Installation

Zur Installation eines DNS-Servers starten Sie YaST und wählen Sie *Software* > *Software-Management* aus. Wählen Sie *Filter* > *Schemata* und schließlich *DHCP- und DNS-Server* aus. Bestätigen Sie die Installation der abhängigen Pakete, um den Installationsvorgang abzuschließen.

21.3 Konfiguration mit YaST

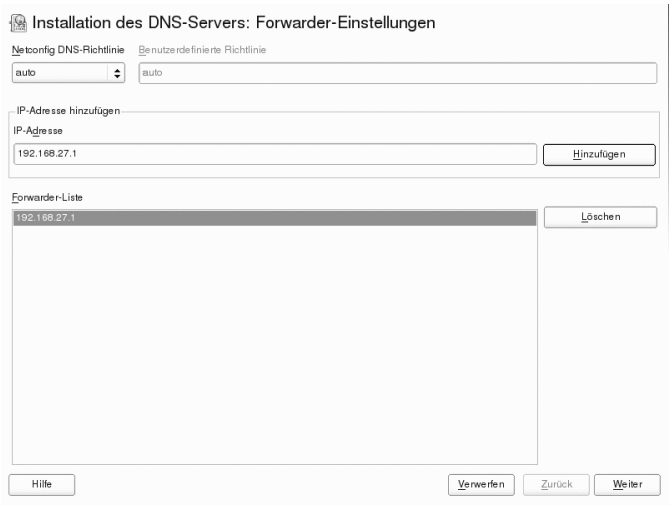
Mit dem DNS-Modul von YaST können Sie einen DNS-Server für Ihr lokales Netzwerk konfigurieren. Beim ersten Starten des Moduls werden Sie von einem Assistenten aufgefordert, einige grundlegende Entscheidungen hinsichtlich der Serveradministration zu treffen. Nach Abschluss der anfänglichen Konfiguration ist eine grundlegende Serverkonfiguration verfügbar, die für einfache Szenarien ausreichend ist. Der Expertenmodus kann für erweiterte Konfigurationsaufgaben verwendet werden, beispielsweise zum Einrichten von ACLs, für Protokollaufgaben, TSIG-Schlüssel und andere Optionen.

21.3.1 Assistentenkonfiguration

Der Assistent besteht aus drei Schritten bzw. Dialogfeldern. An den entsprechenden Stellen in den Dialogfeldern haben Sie die Möglichkeit, in den Expertenkonfigurationsmodus zu wechseln.

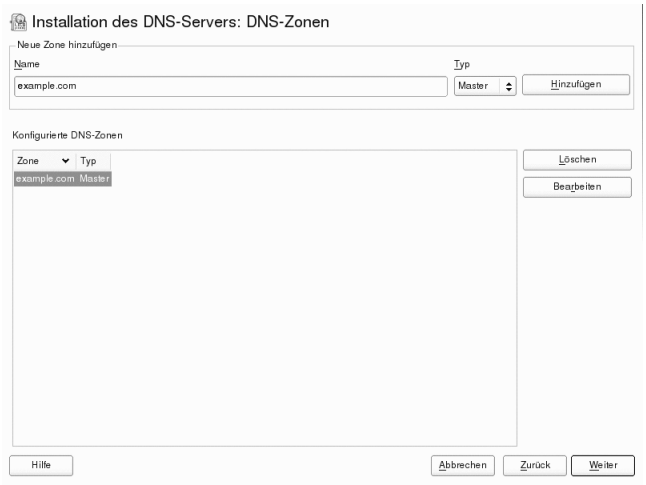
1. Wenn Sie das Modul zum ersten Mal starten, wird das Dialogfeld *Forwarder-Einstellungen* (siehe Abbildung 21.1, „DNS-Server-Installation: Forwarder-Einstellungen“ (S. 316)) geöffnet. Die *Netconfig DNS-Richtlinie* entscheidet darüber, welche Geräte Forwarder zur Verfügung stellen sollten oder ob Sie Ihre eigene *Forwarder-Liste* bereitstellen. Weitere Informationen über netconfig finden Sie auf `man 8 netconfig`.

Abbildung 21.1 *DNS-Server-Installation: Forwarder-Einstellungen*



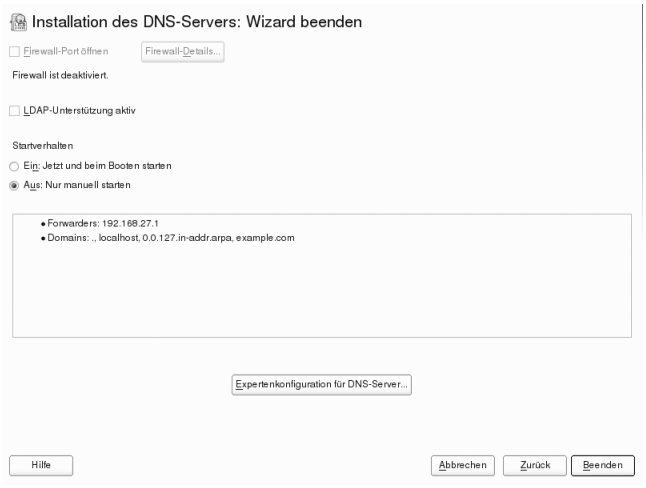
2 Das Dialogfeld *DNS-Zonen* besteht aus mehreren Teilen und ist für die Verwaltung von Zonendateien zuständig, wie in Abschnitt 21.6, „Zonendateien“ (S. 332) beschrieben. Bei einer neuen Zone müssen Sie unter *Name der Zone* einen Namen angeben. Um eine Reverse Zone hinzuzufügen, muss der Name auf `.in-addr.arpa` enden. Wählen Sie schließlich den *Zonentyp* (Master oder Slave) aus. Weitere Informationen hierzu finden Sie unter Abbildung 21.2, „DNS-Server-Installation: DNS-Zonen“ (S. 317). Klicken Sie auf *Zone bearbeiten*, um andere Einstellungen für eine bestehende Zone zu konfigurieren. Zum Entfernen einer Zone klicken Sie auf *Zone löschen*.

Abbildung 21.2 *DNS-Server-Installation: DNS-Zonen*



3 Im letzten Dialogfeld können Sie den DNS-Port in der Firewall öffnen, indem Sie auf *Firewall-Port öffnen* klicken. Legen Sie dann fest, ob der DNS-Server gestartet werden soll (*Ein* oder *Aus*). Außerdem können Sie die LDAP-Unterstützung aktivieren. Weitere Informationen hierzu finden Sie unter Abbildung 21.3, „DNS-Server-Installation: Wizard beenden“ (S. 317).

Abbildung 21.3 *DNS-Server-Installation: Wizard beenden*



21.3.2 Konfiguration für Experten

Nach dem Starten des Moduls öffnet YaST ein Fenster, in dem mehrere Konfigurationsoptionen angezeigt werden. Nach Abschluss dieses Fensters steht eine DNS-Server-Konfiguration mit Grundfunktionen zur Verfügung:

Start

Legen Sie unter *Start* fest, ob der DNS-Server beim Booten des Systems oder manuell gestartet werden soll. Um den DNS-Server sofort zu starten, wählen Sie *DNS-Server nun starten*. Um den DNS-Server anzuhalten, wählen Sie *DNS-Server nun anhalten*. Zum Speichern der aktuellen Einstellungen wählen Sie *Einstellungen speichern und DNS-Server nun neu starten*. Sie können den DNS-Anschluss in der Firewall mit *Firewall-Port öffnen* öffnen und die Firewall-Einstellungen mit *Firewall-Details* bearbeiten.

Wenn Sie *LDAP-Unterstützung aktiv* wählen, werden die Zone-Dateien von einer LDAP-Datenbank verwaltet. Alle Änderungen an Zonendaten, die in der LDAP-Datenbank gespeichert werden, werden vom DNS-Server gleich nach dem Neustart erfasst oder er wird aufgefordert, seine Konfiguration neu zu laden.

Forwarder

Falls Ihr lokaler DNS-Server eine Anforderung nicht beantworten kann, versucht er, diese Anforderung an einen *Forwarder* weiterzuleiten, falls dies so konfiguriert wurde. Dieser Forwarder kann manuell zur *Forwarder-Liste* hinzugefügt werden. Wenn der Forwarder nicht wie bei Einwahlverbindungen statisch ist, wird die Konfiguration von *netconfig* verarbeitet. Weitere Informationen über netconfig finden Sie auf `man 8 netconfig`. Server

Grundlegende Optionen

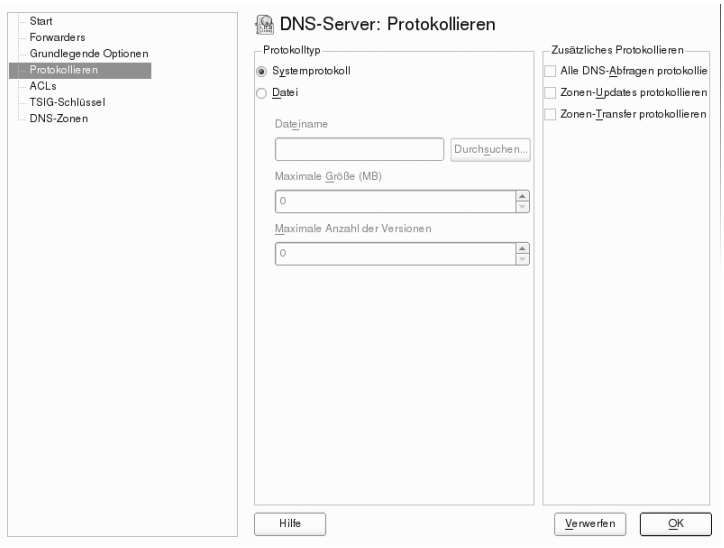
In diesem Abschnitt werden grundlegende Serveroptionen festgelegt. Wählen Sie im Menü *Option* das gewünschte Element und geben Sie dann den Wert im entsprechenden Eintragsfeld an. Nehmen Sie den neuen Eintrag auf, indem Sie auf *Hinzufügen* klicken.

Protokollierung

Um festzulegen, was und wie der DNS-Server protokollieren soll, wählen Sie *Protokollieren* aus. Geben Sie unter *Protokolltyp* an, wohin der DNS-Server die Protokolldaten schreiben soll. Verwenden Sie die systemweite Protokolldatei `/var/log/messages`, indem Sie *Systemprotokoll* auswählen oder geben Sie eine andere Datei an, indem Sie *Datei* auswählen. In letzterem Fall müssen Sie außerdem einen Namen, die maximale Dateigröße in Megabyte und die Anzahl der zu speichernden Versionen von Protokolldateien angeben.

Weitere Optionen sind unter *Zusätzliches Protokollieren* verfügbar. Durch Aktivieren von *Alle DNS-Abfragen protokollieren* wird *jede* Abfrage protokolliert. In diesem Fall kann die Protokolldatei extrem groß werden. Daher sollte diese Option nur zur Fehlersuche aktiviert werden. Um den Datenverkehr zu protokollieren, der während Zonenaktualisierungen zwischen dem DHCP- und dem DNS-Server stattfindet, aktivieren Sie *Zonen-Updates protokollieren*. Um den Datenverkehr während eines Zonentransfers von Master zu Slave zu protokollieren, aktivieren Sie *Zonen-Transfer protokollieren*. Weitere Informationen hierzu finden Sie unter Abbildung 21.4, „DNS-Server: Protokollieren“ (S. 319).

Abbildung 21.4 *DNS-Server: Protokollieren*



Verwenden von ACLs

In diesem Fenster legen Sie ACLs (Access Control Lists = Zugriffssteuerungslisten) fest, mit denen Sie den Zugriff einschränken. Nach der Eingabe eines eindeutigen Namens unter *Name* geben Sie unter *Wert* eine IP-Adresse (mit oder ohne Netzmaske) wie folgt an:

```
{ 192.168.1/24; }
```

Die Syntax der Konfigurationsdatei erfordert, dass die Adresse mit einem Strichpunkt endet und in geschwungenen Klammern steht.

TSIG-Schlüssel

Der Hauptzweck von TSIG-Schlüsseln (Transaction Signatures = Transaktionssignaturen) ist die Sicherung der Kommunikation zwischen DHCP- und DNS-Servern. Diese werden unter Abschnitt 21.8, „Sichere Transaktionen“ (S. 337) beschrieben.

Zum Erstellen eines TSIG-Schlüssels geben Sie einen eindeutigen Namen im Feld mit der Beschriftung *Schlüssel-ID* ein und geben die Datei an, in der der Schlüssel gespeichert werden soll (*Dateiname*). Bestätigen Sie Ihre Einstellung mit *Hinzufügen*.

Wenn Sie einen vorher erstellten Schlüssel verwenden möchten, lassen Sie das Feld *Schlüssel-ID* leer und wählen die Datei, in der der gewünschten Schlüssel gespeichert wurde unter *Dateiname*. Dann bestätigen Sie die Auswahl mit *Hinzufügen*.

Hinzufügen einer Slave-Zone

Wenn Sie eine Slave-Zone hinzufügen möchten, klicken Sie auf *DNS-Zonen*, wählen Sie den Zonentyp *Slave* aus, geben Sie den Namen der neuen Zone ein und klicken Sie auf *Hinzufügen*.

Geben Sie im *Zonen-Editor* unter *IP des Master DNS-Servers* den Master an, von dem der Slave die Daten abrufen soll. Um den Zugriff auf den Server zu beschränken, wählen Sie eine der ACLs aus der Liste aus.

Hinzufügen einer Masterzone

Wenn Sie eine Masterzone hinzufügen möchten, klicken Sie auf *DNS-Zonen*, wählen Sie den Zonentyp *Master* aus, geben Sie den Namen der neuen Zone ein und klicken Sie auf *Hinzufügen*. Beim Hinzufügen einer Masterzone ist auch eine Reverse Zone erforderlich. Wenn Sie beispielsweise die Zone `example.com` hinzufügen, die auf Hosts in einem Subnetz `192.168.1.0/24` zeigt, sollten Sie auch eine Reverse Zone für den betreffenden IP-Adressbereich erstellen. Per Definition sollte dieser den Namen `1.168.192.in-addr.arpa` erhalten.

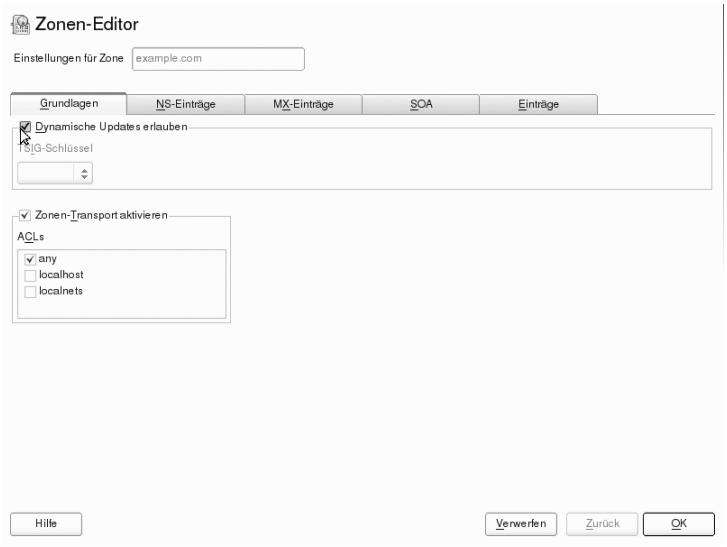
Bearbeiten einer Masterzone

Wenn Sie eine Masterzone bearbeiten möchten, klicken Sie auf *DNS-Zonen*, wählen Sie die Masterzone in der Tabelle aus und klicken Sie auf *Bearbeiten*. Dieses Dialogfeld besteht aus mehreren Seiten: *Grundlagen* (die zuerst geöffnete Seite), *DNS-Einträge*, *MX-Einträge*, *SOA* und *Einträge*.

Im grundlegenden Dialogfeld in Abbildung 21.5, „DNS-Server: Zonen-Editor (Basis)“ (S. 322) können Sie die Einstellungen für das dynamische DNS festlegen und auf Optionen für Zonentransfers an Clients und Slave-Namenserver zugreifen. Zum Zulassen dynamischer Aktualisierungen der Zonen wählen Sie *Dynamische Updates erlauben* und wählen Sie dann den entsprechenden TSIG-Schlüssel aus. Der Schlüssel muss definiert werden, bevor die Aktualisierung startet. Zum Aktivieren der Zonentransfers wählen Sie die entsprechenden ACLs. ACLs müssen bereits definiert sein.

Wählen Sie in diesem Basisdialog, ob Zonen-Transfers aktiviert werden sollen. Verwenden Sie die aufgelisteten ACLs, um festzulegen, wer Zonen herunterladen kann.

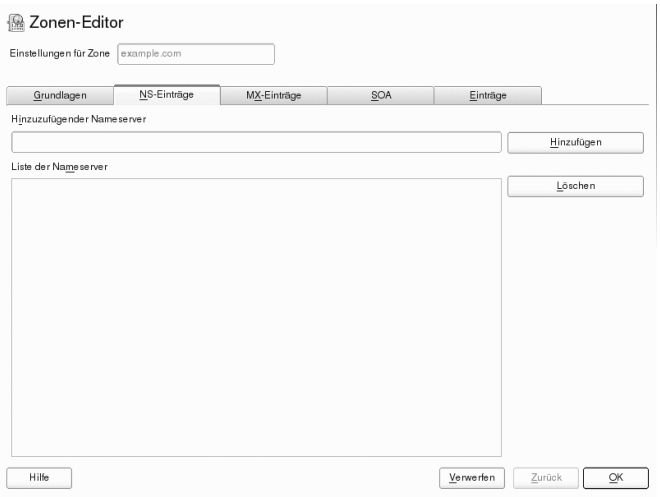
Abbildung 21.5 *DNS-Server: Zonen-Editor (Basis)*



Zonen-Editor (NS-Einträge)

In diesem Dialogfeld können Sie alternative Namenserver für die angegebenen Zonen definieren. Vergewissern Sie sich, dass Ihr eigener Namenserver in der Liste enthalten ist. Um einen Eintrag hinzuzufügen, geben Sie seinen Namen unter *Hinzuzufügender Namenserver* ein und bestätigen Sie den Vorgang anschließend mit *Hinzufügen*. Weitere Informationen hierzu finden Sie unter Abbildung 21.6, „DNS-Server: Zonen-Editor (DNS-Einträge)“ (S. 323).

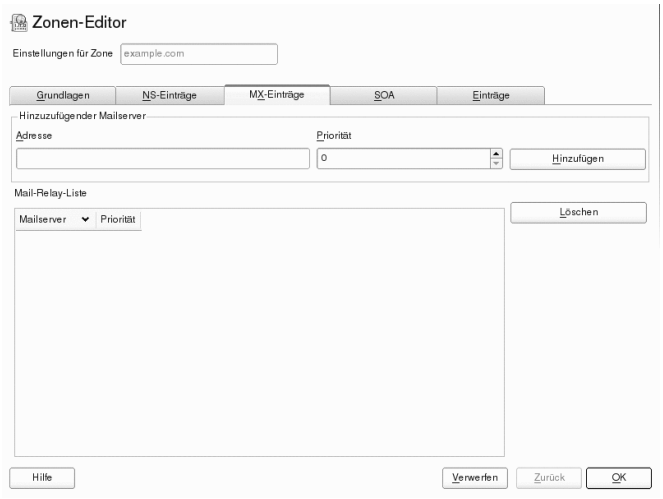
Abbildung 21.6 *DNS-Server: Zonen-Editor (DNS-Einträge)*



Zonen-Editor (MX-Einträge)

Um einen Mailserver für die aktuelle Zone zur bestehenden Liste hinzuzufügen, geben Sie die entsprechende Adresse und den entsprechenden Prioritätswert ein. Bestätigen Sie den Vorgang anschließend durch Auswahl von *Hinzufügen*. Weitere Informationen hierzu finden Sie unter Abbildung 21.7, „DNS-Server: Zonen-Editor (MX-Einträge)“ (S. 324).

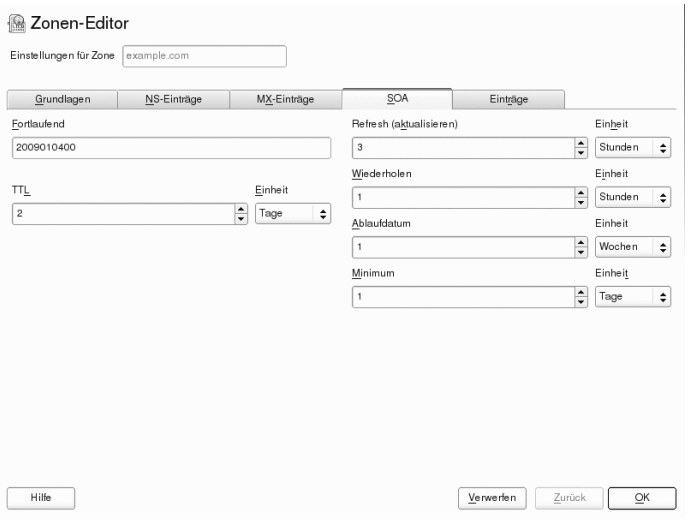
Abbildung 21.7 *DNS-Server: Zonen-Editor (MX-Einträge)*



Zonen-Editor (SOA)

Auf dieser Seite können Sie SOA (Start of Authority)-Einträge erstellen. Eine Erklärung der einzelnen Optionen finden Sie in Beispiel 21.6, „Datei /var/lib/named/example.com.zone“ (S. 333). Das Ändern von SOA-Datensätzen wird für dynamischen Zonen, die über LDAP verwaltet werden, nicht unterstützt.

Abbildung 21.8 *DNS-Server: Zonen-Editor (SOA)*



Zonen-Editor (Einträge)

In diesem Dialogfeld wird die Namenauflösung verwaltet. Geben Sie unter *Eintragschlüssel* den Hostnamen an und wählen Sie anschließend den Typ aus. *A-Record* steht für den Haupteintrag. Der Wert hierfür sollte eine IP-Adresse sein. *CNAME* ist ein Alias. Verwenden Sie die Typen *NS* und *MX* für detaillierte oder partielle Einträge, mit denen die Informationen aus den Registerkarten *NS-Einträge* und *MX-Einträge* erweitert werden. Diese drei Typen werden in einen bestehenden A-Eintrag aufgelöst. *PTR* dient für Reverse Zones. Es handelt sich um das Gegenteil eines `A`-Eintrags, wie zum Beispiel:

```
hostname.example.com. IN A 192.168.0.1
1.0.168.192.in-addr.arpa IN PTR hostname.example.com.
```

ANMERKUNG: Bearbeiten der Reverse Zone

Wechseln Sie nach dem Hinzufügen einer Forward Zone wieder in das Hauptmenü und wählen Sie die Reverse Zone zur Bearbeitung aus. Markieren Sie im Karteireiter *Grundlagen* das Kontrollkästchen *Einträge automatisch generieren aus* und wählen Sie Ihre Forward Zone aus. Auf diese Weise werden alle Änderungen an der Forward Zone automatisch in der Reverse Zone aktualisiert.

21.4 Starten des Namenservers BIND

Bei SUSE® Linux Enterprise Server-Systemen ist der Namenserver BIND (*Berkeley Internet Name Domain*) vorkonfiguriert, sodass er problemlos unmittelbar nach der Installation gestartet werden kann. Wenn Sie bereits über eine funktionierende Internetverbindung verfügen und `127.0.0.1` als Namenserveradresse für `localhost` in `/etc/resolv.conf` eingegeben haben, verfügen Sie normalerweise bereits über eine funktionierende Namenauflösung, ohne dass Ihnen der DNS des Anbieters bekannt sein muss. BIND führt die Namenauflösung über den Root-Namenserver durch. Dies ist ein wesentlich langsamerer Prozess. Normalerweise sollte der DNS des Anbieters zusammen mit der zugehörigen IP-Adresse in die Konfigurationsdatei `/etc/named.conf` unter `forwarders` eingegeben werden, um eine effektive und sichere Namenauflösung zu gewährleisten. Wenn dies so weit funktioniert, wird der Namenserver als reiner *Nur-Cache*-Namenserver ausgeführt. Nur wenn Sie seine eigenen Zonen konfigurieren, wird er ein richtiger DNS. Ein einfaches Beispiel hierfür ist in der Dokumentation unter `/usr/share/doc/packages/bind/config` enthalten.

TIPP: Automatische Anpassung der Namenserverinformationen

Je nach Typ der Internet- bzw. Netzwerkverbindung können die Namenserverinformationen automatisch an die aktuellen Bedingungen angepasst werden. Setzen Sie hierfür die Variable `MODIFY_NAMED_CONF_DYNAMICALLY` in der Datei `/etc/sysconfig/network/config` auf `yes`.

Richten Sie jedoch noch keine offiziellen Domänen ein. Warten Sie, bis Ihnen eine von der verantwortlichen Institution zugewiesen wird. Selbst wenn Sie eine eigene Domäne besitzen und diese vom Anbieter verwaltet wird, sollten Sie sie besser nicht verwenden, da BIND ansonsten keine Anforderungen für diese Domäne weiterleitet. Beispielsweise könnte in diesem Fall für diese Domäne der Zugriff auf den Webserver beim Anbieter nicht möglich sein.

Geben Sie zum Starten des Namenservers den Befehl `rcnamedstart` als `root` ein. Falls rechts in grüner Schrift "done" angezeigt wird, wurde named, wie der Namenserverprozess hier genannt wird, erfolgreich gestartet. Testen Sie den Namenserver umgehend auf dem lokalen System mit den Programmen `host` oder `dig`. Sie sollten `localhost` als Standardserver mit der Adresse `127.0.0.1` zurückgeben. Ist dies nicht der Fall, enthält `/etc/resolv.conf` einen falschen Namenservereintrag oder die Datei ist nicht vorhanden. Geben Sie beim ersten Test `host 127.0.0.1` ein.

Dieser Eintrag sollte immer funktionieren. Wenn Sie eine Fehlermeldung erhalten, prüfen Sie mit `rcnamed status`, ob der Server tatsächlich ausgeführt wird. Wenn der Namenserver sich nicht starten lässt oder unerwartetes Verhalten zeigt, finden Sie die Ursache normalerweise in der Protokolldatei `/var/log/messages`.

Um den Namenserver des Anbieters oder einen bereits in Ihrem Netzwerk ausgeführten Server als Forwarder zu verwenden, geben Sie die entsprechende IP-Adresse(n) im Abschnitt `options` unter `forwarders` ein. Bei den Adressen in Beispiel 21.1, „Weiterleitungsoptionen in named.conf“ (S. 327) handelt es sich lediglich um Beispiele. Passen Sie diese Einträge an Ihr eigenes Setup an.

Beispiel 21.1 *Weiterleitungsoptionen in named.conf*

```
options {
        directory "/var/lib/named";
        forwarders { 10.11.12.13; 10.11.12.14; };
        listen-on { 127.0.0.1; 192.168.1.116; };
        allow-query { 127/8; 192.168/16 };
        notify no;
        };
```

Auf den Eintrag `options` folgen Einträge für die Zone, `localhost` und `0.0.127.in-addr.arpa`. Der Eintrag `type hint` unter. sollte immer vorhanden sein. Die entsprechenden Dateien müssen nicht bearbeitet werden und sollten so funktionieren, wie sie sind. Achten Sie außerdem darauf, dass jeder Eintrag mit einem; abgeschlossen ist und dass sich die geschweiften Klammern an der richtigen Position befinden. Wenn Sie die Konfigurationsdatei `/etc/named.conf` oder die Zonendateien geändert haben, teilen Sie BIND mit, die Datei erneut zu lesen. Verwenden Sie hierfür den Befehl `rcnamedreload`. Sie erzielen dasselbe Ergebnis, wenn Sie den Namenserver mit `rcnamedrestart` stoppen und erneut starten. Sie können den Server durch Eingabe von `rcnamedstop` jederzeit stoppen.

21.5 Die Konfigurationsdatei /etc/dhcpd.conf

Alle Einstellungen für den BIND-Namenserver selbst sind in der Datei `/etc/named.conf` gespeichert. Die Zonendaten für die zu bearbeitenden Domänen, die aus Hostnamen, IP-Adressen usw. bestehen, sind jedoch in gesonderten Dateien im Verzeichnis `/var/lib/named` gespeichert. Einzelheiten hierzu werden weiter unten beschrieben.

/etc/named.conf lässt sich grob in zwei Bereiche untergliedern. Der eine ist der Abschnitt options für allgemeine Einstellungen und der zweite besteht aus zone-Einträgen für die einzelnen Domänen. Der Abschnitt logging und die Einträge unter acl (access control list, Zugriffssteuerungsliste) sind optional. Kommentarzeilen beginnen mit # oder mit //. Eine Minimalversion von /etc/named.conf finden Sie in Beispiel 21.2, „Eine Grundversion von /etc/named.conf“ (S. 328).

Beispiel 21.2 *Eine Grundversion von /etc/named.conf*

```
options {
        directory "/var/lib/named";
        forwarders { 10.0.0.1; };
        notify no;
};

zone "localhost" in {
       type master;
       file "localhost.zone";
};

zone "0.0.127.in-addr.arpa" in {
        type master;
        file "127.0.0.zone";
};

zone "." in {
        type hint;
        file "root.hint";
};
```

21.5.1 Wichtige Konfigurationsoptionen

directory "*Dateiname*";
: Gibt das Verzeichnis an, in dem BIND die Dateien mit den Zonendaten finden kann. In der Regel ist dies /var/lib/named.

forwarders { *ip-adresse*; };
: Gibt die Namenserver (zumeist des Anbieters) an, an die DNS-Anforderungen weitergeleitet werden sollen, wenn sie nicht direkt aufgelöst werden können. Ersetzen Sie *IP-Adresse* durch eine IP-Adresse wie 192.168.1.116.

forward first;
: Führt dazu, dass DNS-Anforderungen weitergeleitet werden, bevor versucht wird, sie über die Root-Namenserver aufzulösen. Anstatt forward first kann

`forward only` verwendet werden. Damit werden alle Anforderungen weitergeleitet, ohne dass sie an die Root-Namenserver gesendet werden. Dies ist bei Firewall-Konfigurationen sinnvoll.

listen-on port 53 { 127.0.0.1; *IP-Adresse*; };
: Informiert BIND darüber, an welchen Netzwerkschnittstellen und Ports Client-Abfragen akzeptiert werden sollen. `port 53` muss nicht explizit angegeben werden, da `53` der Standardport ist. Geben Sie `127.0.0.1` ein, um Anforderungen vom lokalen Host zuzulassen. Wenn Sie diesen Eintrag ganz auslassen, werden standardmäßig alle Schnittstellen verwendet.

listen-on-v6 port 53 {any; };
: Informiert BIND darüber, welcher Port auf IPv6-Client-Anforderungen überwacht werden soll. Die einzige Alternative zu `any` ist `none`. Bei IPv6 akzeptiert der Server nur Wildcard-Adressen.

query-source address * port 53;
: Dieser Eintrag ist erforderlich, wenn eine Firewall ausgehende DNS-Anforderungen blockiert. Dadurch wird BIND angewiesen, Anforderungen extern von Port 53 und nicht von einem der Ports mit den hohen Nummern über 1024 aufzugeben.

query-source-v6 address * port 53;
: Informiert BIND darüber, welcher Port für IPv6-Abfragen verwendet werden soll.

allow-query { 127.0.0.1; *net*; };
: Definiert die Netzwerke, von denen aus Clients DNS-Anforderungen aufgeben können. Ersetzen Sie *Netz* durch Adressinformationen wie `192.168.2.0/24`. Der Wert `/24` am Ende ist ein abgekürzter Ausdruck für die Netzmaske, hier `255.255.255.0`.

allow-transfer ! *;;
: Legt fest, welche Hosts Zonentransfers anfordern können. Im vorliegenden Beispiel werden solche Anforderungen mit `! *` vollständig verweigert. Ohne diesen Eintrag können Zonentransfer ohne Einschränkungen von jedem beliebigen Ort aus angefordert werden.

statistics-interval 0;
: Ohne diesen Eintrag generiert BIND in der Datei `/var/log/messages` pro Stunde mehrere Zeilen mit statistischen Informationen. Setzen Sie diesen Wert auf

"0", um diese Statistiken vollständig zu unterdrücken, oder legen Sie ein Zeitintervall in Minuten fest.

cleaning-interval 720;
: Diese Option legt fest, in welchen Zeitabständen BIND den Cache leert. Jedes Mal, wenn dies geschieht, wird ein Eintrag in `/var/log/messages` ausgelöst. Die verwendete Einheit für die Zeitangabe ist Minuten. Der Standardwert ist 60 Minuten.

interface-interval 0;
: BIND durchsucht die Netzwerkschnittstellen regelmäßig nach neuen oder nicht vorhandenen Schnittstellen. Wenn dieser Wert auf `0` gesetzt ist, wird dieser Vorgang nicht durchgeführt und BIND überwacht nur die beim Start erkannten Schnittstellen. Anderenfalls wird das Zeitintervall in Minuten angegeben. Der Standardwert ist 60 Minuten.

notify no;
: `no` verhindert, dass anderen Namenserver informiert werden, wenn Änderungen an den Zonendaten vorgenommen werden oder wenn der Namenserver neu gestartet wird.

Eine Liste der verfügbaren Optionen finden Sie auf der man-Seite `man 5 named.conf`.

21.5.2 Protokollierung

Der Umfang, die Art und Weise und der Ort der Protokollierung kann in BIND extensiv konfiguriert werden. Normalerweise sollten die Standardeinstellungen ausreichen. In Beispiel 21.3, „Eintrag zur Deaktivierung der Protokollierung“ (S. 330) sehen Sie die einfachste Form eines solchen Eintrags, bei dem jegliche Protokollierung unterdrückt wird.

Beispiel 21.3 *Eintrag zur Deaktivierung der Protokollierung*

```
logging {
        category default { null; };
};
```

21.5.3 Zoneneinträge

Beispiel 21.4 *Zoneneintrag für "example.com"*

```
zone "example.com" in {
      type master;
      file "example.com.zone";
      notify no;
};
```

Geben Sie nach `zone` den Namen der zu verwaltenden Domäne (`example.com`) an, gefolgt von `in` und einem Block relevanter Optionen in geschweiften Klammern, wie in Beispiel 21.4, „Zoneneintrag für "example.com"“ (S. 331) gezeigt. Um eine *Slave-Zone* zu definieren, ändern Sie den Wert von `type` in `slave` und geben Sie einen Namenserver an, der diese Zone als `master` verwaltet (dieser kann wiederum ein Slave eines anderen Masters sein), wie in Beispiel 21.5, „Zoneneintrag für "example.net"“ (S. 331) gezeigt.

Beispiel 21.5 *Zoneneintrag für "example.net"*

```
zone "example.net" in {
      type slave;
      file "slave/example.net.zone";
      masters { 10.0.0.1; };
};
```

Zonenoptionen:

type master;
: Durch die Angabe `master` wird BIND darüber informiert, dass der lokale Namenserver für die Zone zuständig ist. Dies setzt voraus, dass eine Zonendatei im richtigen Format erstellt wurde.

type slave;
: Diese Zone wird von einem anderen Namenserver übertragen. Sie muss zusammen mit `masters` verwendet werden.

type hint;
: Die Zone `.` vom Typ `hint` wird verwendet, um den root-Namenserver festzulegen. Diese Zonendefinition kann unverändert beibehalten werden.

Datei `example.com.zone` oder Datei "slave/example.net.zone";
: In diesem Eintrag wird die Datei angegeben, in der sich die Zonendaten für die Domäne befinden. Diese Datei ist für einen Slave nicht erforderlich, da die betreffenden Daten von einem anderen Namenserver abgerufen werden. Um zwischen Master- und Slave-Dateien zu unterscheiden, verwenden Sie das Verzeichnis `slave` für die Slave-Dateien.

masters { *`server-ip-adresse`*; };
: Dieser Eintrag ist nur für Slave-Zonen erforderlich. Er gibt an, von welchem Namenserver die Zonendatei übertragen werden soll.

allow-update {! *; };
: Mit dieser Option wird der externe Schreibzugriff gesteuert, der Clients das Anlegen von DNS-Einträgen gestattet. Aus Sicherheitsgründen wird davon abgeraten, den Clients Schreibzugriff zu gewähren. Ohne diesen Eintrag sind überhaupt keine Zonenaktualisierungen zulässig. Der oben stehende Eintrag hat dieselbe Wirkung, da `! *` solche Aktivitäten effektiv unterbindet.

21.6 Zonendateien

Zwei Arten von Zonendateien sind erforderlich. Eine Art ordnet IP-Adressen Hostnamen zu, die andere stellt Hostnamen für IP-Adressen bereit.

TIPP: Verwenden des Punktes in Zonendateien

Die . hat eine wichtige Bedeutung in den Zonendateien. Wenn Hostnamen ohne . am Ende angegeben werden, wird die Zone angefügt. Vollständige Hostnamen, die mit einem vollständigen Domänennamen angegeben werden, müssen mit . abgeschlossen werden, um zu verhindern, dass die Domäne ein weiteres Mal angefügt wird. Ein fehlender oder falsch platzierter Punkt ist wahrscheinlich die häufigste Ursache von Fehlern bei der Namenserverkonfiguration.

Der erste zu betrachtende Fall ist die Zonendatei `example.com.zone`, die für die Domäne `example.com` zuständig ist (siehe Beispiel 21.6, „Datei /var/lib/named/example.com.zone“ (S. 333)).

Beispiel 21.6 *Datei /var/lib/named/example.com.zone*

```
1.  $TTL 2D
2.  example.com. IN SOA      dns  root.example.com. (
3.               2003072441  ; serial
4.               1D          ; refresh
5.               2H          ; retry
6.               1W          ; expiry
7.               2D )        ; minimum
8.
9.               IN NS       dns
10.              IN MX       10 mail
11.
12. gate         IN A        192.168.5.1
13.              IN A        10.0.0.1
14. dns          IN A        192.168.1.116
15. mail         IN A        192.168.3.108
16. jupiter      IN A        192.168.2.100
17. venus        IN A        192.168.2.101
18. saturn       IN A        192.168.2.102
19. mercury      IN A        192.168.2.103
20. ntp          IN CNAME    dns
21. dns6         IN A6  0    2002:c0a8:174::
```

Zeile 1:

`$TTL` legt die Standardlebensdauer fest, die für alle Einträge in dieser Datei gelten soll. In diesem Beispiel sind die Einträge zwei Tage lang gültig (`2 D`).

Zeile 2:

Hier beginnt der SOA (Start of Authority)-Steuereintrag:

- Der Name der zu verwaltenden Datei ist `example.com` an der ersten Stelle. Dieser Eintrag endet mit `.`, da anderenfalls die Zone ein zweites Mal angefügt würde. Alternativ kann hier `@` eingegeben werden. In diesem Fall wird die Zone aus dem entsprechenden Eintrag in `/etc/named.conf` extrahiert.

- Nach `IN SOA` befindet sich der Name des Namenservers, der als Master für diese Zone fungiert. Der Name wird von `dns` zu `dns.example.com` erweitert, da er nicht mit `.` endet.

- Es folgt die E-Mail-Adresse der für diesen Namenserver zuständigen Person. Da das Zeichen `@` bereits eine besondere Bedeutung hat, wird hier stattdessen `.` eingegeben. Für `root@example.com` muss der Eintrag wie folgt lauten: `root.example.com.`. Der Punkt `.` muss angehängt werden, damit die Zone nicht hinzugefügt wird.

- Durch `(` werden alle Zeilen bis einschließlich `)` in den SOA-Eintrag aufgenommen.

Zeile 3:

Die Seriennummer (`serial`) ist eine beliebige Nummer, die sich bei jeder Änderung der Datei erhöht. Sie wird benötigt, um die sekundären Namenserver (Slave-Server) über Änderungen zu informieren. Hierfür hat sich eine 10-stellige Nummer aus Datum und Ausführungsnummer in der Form JJJJMMMTTNN als übliches Format etabliert.

Zeile 4:

Die Aktualisierungsrate (`refresh rate`) gibt das Zeitintervall an, in dem die sekundären Namenserver die Seriennummer (`serial`) der Zone überprüfen. In diesem Fall beträgt dieses Intervall einen Tag.

Zeile 5:

Die Wiederholungsrate (`retry`) gibt das Zeitintervall an, nach dem ein sekundärer Namenserver bei einem Fehler erneut versucht, Kontakt zum primären Server herzustellen. In diesem Fall sind dies zwei Stunden.

Zeile 6:

Die Ablaufzeit (`expiry`) gibt den Zeitraum an, nach dem ein sekundärer Server die im Cache gespeicherten Daten verwirft, wenn er keinen erneuten Kontakt zum primären Server herstellen konnte. In diesem Fall ist dies eine Woche.

Zeile 7:

Die letzte Angabe im SOA-Eintrag gibt die negative Cache-Lebensdauer (`negative caching TTL`) an. Sie legt fest, wie lange Ergebnisse nicht aufgelöster DNS-Abfragen anderer Server im Cache gespeichert werden können.

Zeile 9:

`IN NS` gibt den für diese Domäne verantwortlichen Namenserver an. `dns` wird zu `dns.example.com` erweitert, da der Eintrag nicht mit einem `endet.` endet. Es können mehrere solcher Zeilen vorhanden sein - eine für den primären und eine für die einzelnen sekundären Namenserver. Wenn `notify` in `/etc/named.conf` nicht auf `no` gesetzt ist, werden alle hier aufgeführten Namenserver über die Änderungen an den Zonendaten informiert.

Zeile 10:

Der MX-Eintrag gibt den Mailserver an, der E-Mails für die Domäne `example.com` annimmt, verarbeitet und weiterleitet. In diesem Beispiel ist dies der Host `mail.example.com`. Die Zahl vor dem Hostnamen ist der Präferenzwert. Wenn mehrere MX-Einträge vorhanden sind, wird zunächst der Mailserver mit dem kleinsten Wert verwendet. Wenn die Mailzustellung an diesen Server nicht möglich ist, wird ein Versuch mit dem nächsthöheren Wert unternommen.

Zeilen 12 – 19:

Dies sind die eigentlichen Adresseinträge, in denen den Hostnamen eine oder mehrere IP-Adressen zugewiesen werden. Die Namen werden hier ohne `.` aufgelistet, da sie ihre Domäne nicht enthalten. Daher wird ihnen allen `example.com` hinzugefügt. Dem Host `gate` werden zwei IP-Adressen zugewiesen, weil er zwei Netzwerkkarten aufweist. Bei jeder traditionellen Hostadresse (IPv4) wird der Eintrag mit `A` gekennzeichnet. Wenn es sich um eine IPv6-Adresse handelt, wird der Eintrag mit `AAAA` gekennzeichnet.

ANMERKUNG: IPv6-Syntax

Die Syntax des IPv6-Eintrags unterscheidet sich geringfügig von der Syntax von IPv4. Aufgrund der Möglichkeit einer Fragmentierung müssen Informationen zu fehlenden Bits vor der Adresse angegeben werden. Um nur die IPv6-Adresse mit dem erforderlichen Wert "0" auszufüllen, fügen Sie an der korrekten Stelle in der Adresse zwei Doppelpunkte hinzu.

```
pluto     AAAA 2345:00C1:CA11::1234:5678:9ABC:DEF0
pluto     AAAA 2345:00D2:DA11::1234:5678:9ABC:DEF0
```

Zeile 20:

Der Alias `ntp` kann zur Adressierung von `dns` (`CNAME` steht für *canonical name* (kanonischer Name)) verwendet werden.

Die Pseudodomäne `in-addr.arpa` wird für Reverse-Lookups zur Auflösung von IP-Adressen in Hostnamen verwendet. Sie wird in umgekehrter Notation an den Netzwerk-Teil der Adresse angehängt. `192.168` wird also in `168.192.in-addr.arpa` aufgelöst. Weitere Informationen hierzu finden Sie unter Beispiel 21.7, „Reverse-Lookup“ (S. 336).

Beispiel 21.7 *Reverse-Lookup*

```
1.  $TTL 2D
2.  168.192.in-addr.arpa.   IN SOA dns.example.com. root.example.com. (
3.                          2003072441      ; serial
4.                          1D              ; refresh
5.                          2H              ; retry
6.                          1W              ; expiry
7.                          2D )            ; minimum
8.
9.                          IN NS           dns.example.com.
10.
11. 1.5                     IN PTR          gate.example.com.
12. 100.3                   IN PTR          www.example.com.
13. 253.2                   IN PTR          cups.example.com.
```

Zeile 1:

$TTL definiert die Standard-TTL, die für alle Einträge hier gilt.

Zeile 2:

Die Konfigurationsdatei muss Reverse-Lookup für das Netzwerk `192.168` aktivieren. Angenommen, die Zone heißt `168.192.in-addr.arpa`, sollte sie nicht zu den Hostnamen hinzugefügt werden. Daher werden alle Hostnamen in ihrer vollständigen Form eingegeben, d. h. mit der Domäne und einem abschließenden Punkt (`.`). Die restlichen Einträge entsprechen den im vorherigen Beispiel (`example.com`) beschriebenen Einträgen.

Zeilen 3 – ;7:

Sehen Sie sich hierzu das Beispiel für `example.com` an.

Zeile 9:
: Diese Zeile gibt wieder den für diese Zone verantwortlichen Namenserver an. Diesmal wird der Name allerdings in vollständiger Form mit Domäne und `.` am Ende eingegeben.

Zeilen 11 – ;13:
: Dies sind die Zeigereinträge, die auf die IP-Adressen auf den entsprechenden Hosts verweisen. Am Anfang der Zeile wird nur der letzte Teil der IP-Adresse eingegeben, ohne `.` am Ende. Wenn daran die Zone angehängt wird (ohne `.in-addr.arpa`), ergibt sich die vollständige IP-Adresse in umgekehrter Reihenfolge.

Normalerweise sollten Zonentransfers zwischen verschiedenen Versionen von BIND problemlos möglich sein.

21.7 Dynamische Aktualisierung von Zonendaten

Der Ausdruck *dynamische Aktualisierung* bezieht sich auf Vorgänge, bei denen Einträge in den Zonendateien eines Masterservers hinzugefügt, geändert oder gelöscht werden. Dieser Mechanismus wird in RFC 2136 beschrieben. Die dynamische Aktualisierung wird individuell für jeden Zoneneintrag durch Hinzufügen einer optionalen `allow-update`- bzw. `update-policy`-Regel konfiguriert. Dynamisch zu aktualisierende Zonen sollten nicht von Hand bearbeitet werden.

Die zu aktualisierenden Einträge werden mit dem Befehl `nsupdate` an den Server übermittelt. Die genaue Syntax dieses Befehls können Sie der man-Seite für nsupdate (`man8 nsupdate`) entnehmen. Aus Sicherheitsgründen sollten solche Aktualisierungen mithilfe von TSIG-Schlüsseln durchgeführt werden, wie in Abschnitt 21.8, „Sichere Transaktionen“ (S. 337) beschrieben.

21.8 Sichere Transaktionen

Sichere Transaktionen können mithilfe von Transaktionssignaturen (TSIGs) durchgeführt werden, die auf gemeinsam genutzten geheimen Schlüsseln (TSIG-Schlüssel) beruhen. In diesem Abschnitt wird die Erstellung und Verwendung solcher Schlüssel beschrieben.

Sichere Transaktionen werden für die Kommunikation zwischen verschiedenen Servern und für die dynamische Aktualisierung von Zonendaten benötigt. Die Zugriffssteuerung von Schlüsseln abhängig zu machen, ist wesentlich sicherer, als sich lediglich auf IP-Adressen zu verlassen.

Erstellen Sie mit dem folgenden Befehl einen TSIG-Schlüssel (genauere Informationen finden Sie unter `mandnssec-keygen`):

```
dnssec-keygen -a hmac-md5 -b 128 -n HOST host1-host2
```

Dadurch werden zwei Schlüssel mit ungefähr folgenden Namen erstellt:

```
Khost1-host2.+157+34265.private Khost1-host2.+157+34265.key
```

Der Schlüssel selbst (eine Zeichenkette, wie beispielsweise `ejIkuCyyGJwwuN3xAteKgg==`) ist in beiden Dateien enthalten. Um ihn für Transaktionen zu verwenden, muss die zweite Datei (`Khost1-host2.+157+34265.key`) auf den entfernten Host übertragen werden, möglichst auf eine sichere Weise (z. B. über SCP). Auf dem entfernten Server muss der Schlüssel in der Datei `/etc/named.conf` enthalten sein, damit eine sichere Kommunikation zwischen `host1` und `host2` möglich ist:

```
key host1-host2. {
 algorithm hmac-md5;
 secret ";ejIkuCyyGJwwuN3xAteKgg==;
};
```

WARNUNG: Dateiberechtigungen von `/etc/named.conf`

Vergewissern Sie sich, dass die Berechtigungen von `/etc/named.conf` ordnungsgemäß eingeschränkt sind. Der Standardwert für diese Datei lautet `0640`, mit `root` als Eigentümer und `named` als Gruppe. Alternativ können Sie die Schlüssel in eine gesonderte Datei mit speziell eingeschränkten Berechtigungen verschieben, die dann aus `/etc/named.conf` eingefügt werden. Zum Einschließen einer externen Datei verwenden Sie:

```
include  "filename"
```

Ersetzen Sie `filename` durch einen absoluten Pfad zu Ihrer Datei mit den Schlüsseln.

Damit Server `host1` den Schlüssel für `host2` verwenden kann (in diesem Beispiel mit der Adresse `10.1.2.3`), muss die Datei `/etc/named.conf` des Servers folgende Regel enthalten:

```
server 10.1.2.3 {
  keys { host1-host2. ;};
};
```

Analoge Einträge müssen in die Konfigurationsdateien von `host2` aufgenommen werden.

Fügen Sie TSIG-Schlüssel für alle ACLs (Access Control Lists, Zugriffssteuerungslisten, nicht zu verwechseln mit Dateisystem-ACLs) hinzu, die für IP-Adressen und -Adressbereiche definiert sind, um Transaktionssicherheit zu gewährleisten. Der entsprechende Eintrag könnte wie folgt aussehen:

```
allow-update { key host1-host2. ;};
```

Dieses Thema wird eingehender im *Referenzhandbuch für BIND-Administratoren* (unter `update-policy`) erörtert.

21.9 DNS-Sicherheit

DNSSEC (DNS-Sicherheit) wird in RFC 2535 beschrieben. Die für DNSSEC verfügbaren Werkzeuge werden im BIND-Handbuch erörtert.

Einer als sicher betrachteten Zone müssen ein oder mehrere Zonenschlüssel zugeordnet sein. Diese werden mit `dnssec-keygen` erstellt, genau wie die Host-Schlüssel. Zurzeit wird der DSA-Verschlüsselungsalgorithmus zum Erstellen dieser Schlüssel verwendet. Die generierten öffentlichen Schlüssel sollten mithilfe einer `$INCLUDE`-Regel in die entsprechende Zonendatei aufgenommen werden.

Mit dem Befehl `dnssec-makekeyset` werden alle erstellten Schlüssel zu einem Satz zusammengefasst, der dann auf sichere Weise in die übergeordnete Zone übertragen werden muss. In der übergeordneten Zone wird der Satz mit `dnssec-signkey` signiert. Die durch diesen Befehl erstellten Dateien werden anschließend verwendet, um die Zonen mit `dnssec-signzone` zu signieren, wodurch wiederum die Dateien erstellt werden, die für die einzelnen Zonen in `/etc/named.conf` aufgenommen werden sollen.

21.10 Weiterführende Informationen

Weitere Informationen können Sie dem *Referenzhandbuch für BIND-Administratoren* aus Paket `bind-doc` entnehmen, das unter `/usr/share/doc/packages/bind/` installiert ist. Außerdem könnten Sie die RFCs zurate ziehen, auf die im Handbuch verwiesen wird, sowie die in BIND enthaltenen man-Seiten. `/usr/share/doc/packages/bind/README.SuSE` enthält aktuelle Informationen zu BIND in SUSE Linux Enterprise Server.

22 DHCP

Das *DHCP* (Dynamic Host Configuration Protocol) dient dazu, Einstellungen in einem Netzwerk zentral von einem Server aus zuzuweisen. Einstellungen müssen also nicht dezentral an einzelnen Arbeitsplatzcomputern konfiguriert werden. Ein für DHCP konfigurierter Host verfügt nicht über eine eigene statische Adresse. Er konfiguriert sich stattdessen vollständig und automatisch nach den Vorgaben des DHCP-Servers. Wenn Sie auf der Client-Seite den NetworkManager verwenden, brauchen Sie den Client überhaupt nicht zu konfigurieren. Das ist nützlich, wenn Sie in wechselnden Umgebungen arbeiten und nur jeweils eine Schnittstelle aktiv ist. Verwenden Sie den NetworkManager nie auf einem Computer, der einen DHCP-Server ausführt.

TIPP: IBM-System z: DHCP-Unterstützung

Auf IBM-&zseries-Plattformen funktioniert DHCP nur bei Schnittstellen, die die OSA- und OSA Express-Netzwerkkarten verwenden. Nur diese Karten verfügen über eine für die Autokonfigurationsfunktionen von DHCP erforderliche MAC-Adresse.

Eine Möglichkeit zur Konfiguration von DHCP-Servern besteht darin, jeden Client mithilfe der Hardwareadresse seiner Netzwerkkarte zu identifizieren (die in den meisten Fällen statisch ist) und anschließend diesen Client bei jeder Verbindung zum Server mit identischen Einstellungen zu versorgen. Zum anderen kann DHCP aber auch so konfiguriert werden, dass der Server jedem Client, der eine Verbindung zu ihm herstellt, eine Adresse aus einem dafür vorgesehenen Adresspool dynamisch zuweist. In diesem Fall versucht der DHCP-Server, dem Client bei jeder Anforderung dieselbe Adresse zuzuweisen - auch über einen längeren Zeitraum hinweg. Das ist nur möglich, wenn die Anzahl der Clients im Netzwerk nicht die Anzahl der Adressen übersteigt.

DHCP erleichtert Systemadministratoren das Leben. Alle (selbst umfangreiche) Änderungen der Netzwerkadressen oder der -konfiguration können zentral in der Konfigurationsdatei des DHCP-Servers vorgenommen werden. Dies ist sehr viel komfortabler als das Neukonfigurieren zahlreicher Arbeitsstationen. Außerdem können vor allem neue Computer sehr einfach in das Netzwerk integriert werden, indem sie aus dem Adresspool eine IP-Adresse zugewiesen bekommen. Das Abrufen der entsprechenden Netzwerkeinstellungen von einem DHCP-Server ist auch besonders interessant für Notebooks, die regelmäßig in unterschiedlichen Netzwerken verwendet werden.

In diesem Kapitel wird der DHCP-Server im gleichen Subnetz wie die Workstations (192.168.2.0/24) mit 192.168.2.1 als Gateway ausgeführt. Er hat die feste IP-Adresse 192.168.2.254 und bedient die beiden Adressbereiche 192.168.2.10 bis 192.168.2.20 und 192.168.2.100 bis 192.168.2.200;.

Neben IP-Adresse und Netzmaske werden dem Client nicht nur der Computer- und Domänenname, sondern auch das zu verwendende Gateway und die Adressen der Namenserver mitgeteilt. Im Übrigen können auch etliche andere Parameter zentral konfiguriert werden, z. B. ein Zeitserver, von dem die Clients die aktuelle Uhrzeit abrufen können, oder ein Druckserver.

22.1 Konfigurieren eines DHCP-Servers mit YaST

WICHTIG: LDAP-Unterstützung

In dieser Version von SUSE Linux Enterprise Server kann das DHCP-Modul von YaST so eingestellt werden, dass die Serverkonfiguration lokal gespeichert wird (auf dem Host, der den DHCP-Server ausführt), oder so, dass die Konfigurationsdaten von einem LDAP-Server verwaltet werden. Wenn Sie LDAP verwenden möchten, müssen Sie vor der Konfiguration des DHCP-Servers die LDAP-Umgebung einrichten.

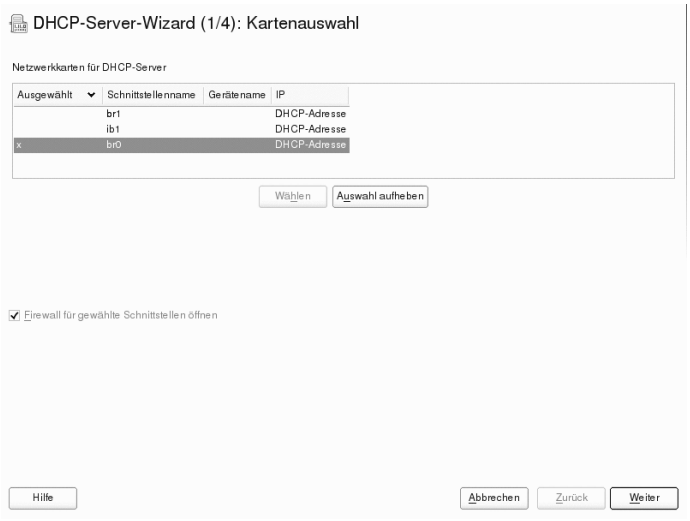
Das DHCP-Modul von YaST ermöglicht die Einrichtung Ihres eigenen DHCP-Servers für das lokale Netzwerk. Das Modul kann im einfachen oder im Expertenmodus ausgeführt werden.

22.1.1 Anfängliche Konfiguration (Assistent)

Beim ersten Starten des Moduls werden Sie von einem Assistenten aufgefordert, einige grundlegende Entscheidungen hinsichtlich der Serveradministration zu treffen. Nach Abschluss der anfänglichen Konfiguration ist eine grundlegende Serverkonfiguration verfügbar, die für einfache Szenarien ausreichend ist. Komplexere Konfigurationsaufgaben können im Expertenmodus ausgeführt werden.

Kartenauswahl
: Im ersten Schritt ermittelt YaST die in Ihr System eingebundenen Netzwerkschnittstellen und zeigt sie anschließend in einer Liste an. Wählen Sie in dieser Liste die Schnittstelle aus, auf der der DHCP-Server lauschen soll, und klicken Sie auf *Hinzufügen*. Wählen Sie anschließend die Option *Firewall für gewählte Schnittstelle öffnen*, um die Firewall für diese Schnittstelle zu öffnen. Weitere Informationen hierzu finden Sie unter Abbildung 22.1, „DHCP-Server: Kartenauswahl“ (S. 343).

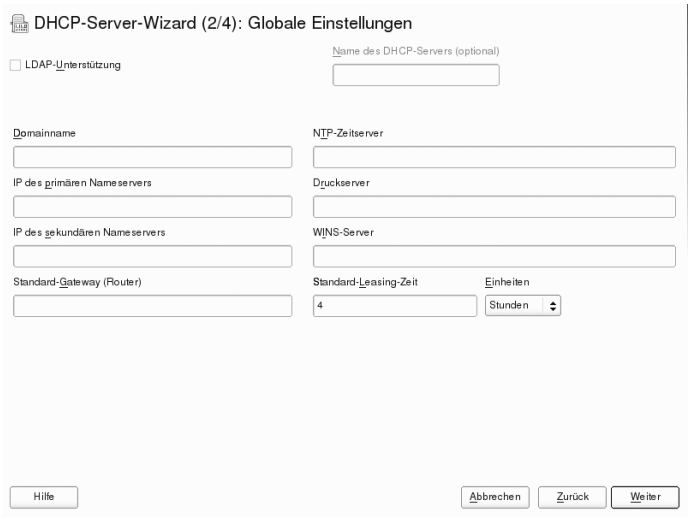
Abbildung 22.1 *DHCP-Server: Kartenauswahl*



Globale Einstellungen
: Geben Sie anhand des Kontrollkästchens an, ob Ihre DHCP-Einstellungen automatisch von einem LDAP-Server gespeichert werden sollen. In den Eingabefeldern legen Sie die Netzwerkinformationen fest, die jeder von diesem DHCP-Server verwaltete Client erhalten soll. Diese sind: Domänenname, Adresse eines Zeitser-

vers, Adressen der primären und sekundären Namenserver, Adressen eines Druck- und WINS-Servers (für gemischte Netzwerkumgebungen mit Windows- und Linux-Clients), Gateway-Adressen und Leasing-Zeit. Weitere Informationen hierzu finden Sie unter Abbildung 22.2, „DHCP-Server: Globale Einstellungen“ (S. 344).

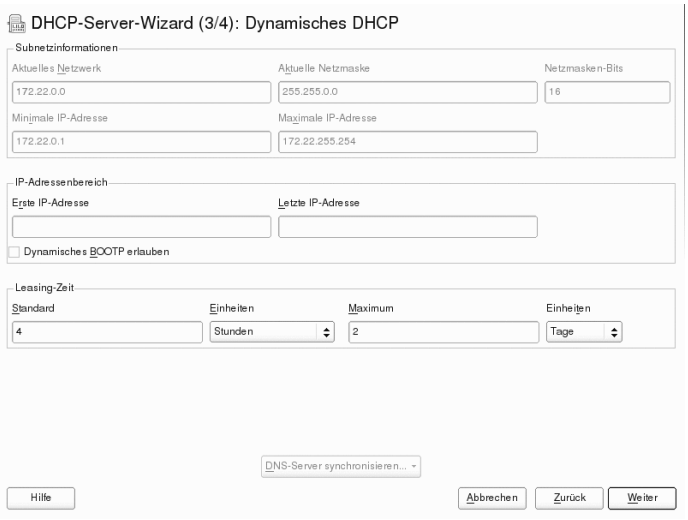
Abbildung 22.2 *DHCP-Server: Globale Einstellungen*



Dynamisches DHCP

In diesem Schritt konfigurieren Sie die Vergabe der dynamischen IP-Adressen an Clients. Hierzu legen Sie einen Bereich von IP-Adressen fest, in dem die zu vergebenden Adressen der DHCP-Clients liegen dürfen. Alle zu vergebenden Adressen müssen unter eine gemeinsame Netzmaske fallen. Legen Sie abschließend die Leasing-Zeit fest, für die ein Client seine IP-Adresse behalten darf, ohne eine Verlängerung der Leasing-Zeit beantragen zu müssen. Legen Sie optional auch die maximale Leasing-Zeit fest, innerhalb derer eine bestimmte IP-Adresse auf dem Server für einen bestimmten Client reserviert bleibt. Weitere Informationen hierzu finden Sie unter Abbildung 22.3, „DHCP-Server: Dynamisches DHCP“ (S. 345).

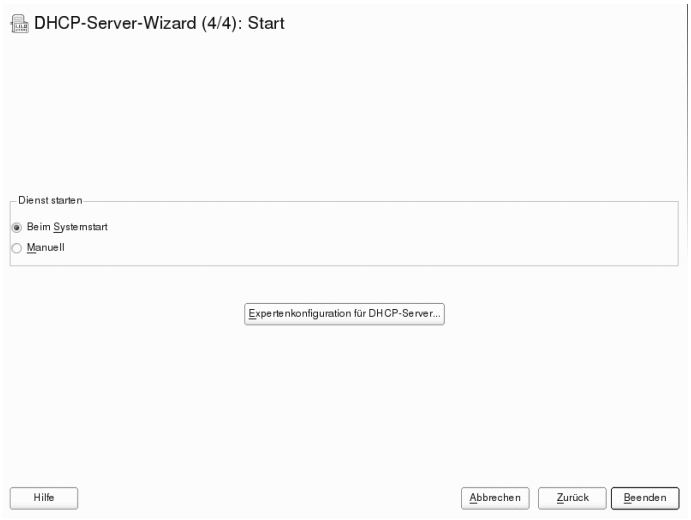
Abbildung 22.3 *DHCP-Server: Dynamisches DHCP*



Fertigstellen der Konfiguration und Auswahl des Startmodus

Nachdem Sie den dritten Teil des Konfigurationsassistenten abgeschlossen haben, gelangen Sie in ein letztes Dialogfeld, das sich mit den Startoptionen des DHCP-Servers befasst. Hier können Sie festlegen, ob der DHCP-Server automatisch beim Booten des Systems oder bei Bedarf (z. B. zu Testzwecken) manuell gestartet werden soll. Klicken Sie auf *Verlassen*, um die Konfiguration des Servers abzuschließen. Weitere Informationen hierzu finden Sie unter Abbildung 22.4, „DHCP-Server: Start“ (S. 346).

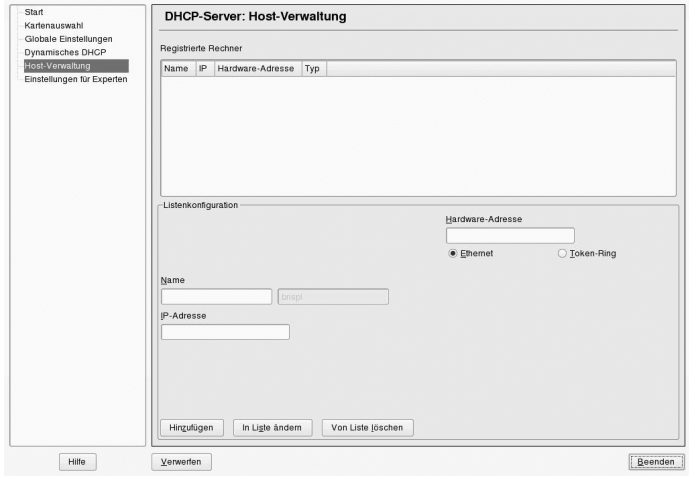
Abbildung 22.4 *DHCP-Server: Start*



Host-Verwaltung

Statt der Verwendung des dynamischen DHCP, wie in den vorigen Abschnitten beschrieben, können Sie den Server auch so konfigurieren, dass Adressen in fast statischer Weise zugewiesen werden. Dafür geben Sie in den Eintragsfeldern im unteren Teil eine Liste der in dieser Art zu verwaltenden Clients ein. Geben Sie vor allem *Name* und *IP-Adresse* für einen solchen Client an, die *Hardware-Adresse* und den *Netzwerktyp* (Token-Ring oder Ethernet). Ändern Sie die oben angezeigte Liste der Clients mit *Hinzufügen*, *Bearbeiten* und *Löschen*. Weitere Informationen hierzu finden Sie unter Abbildung 22.5, „DHCP-Server: Host-Verwaltung“ (S. 347).

Abbildung 22.5 *DHCP-Server: Host-Verwaltung*

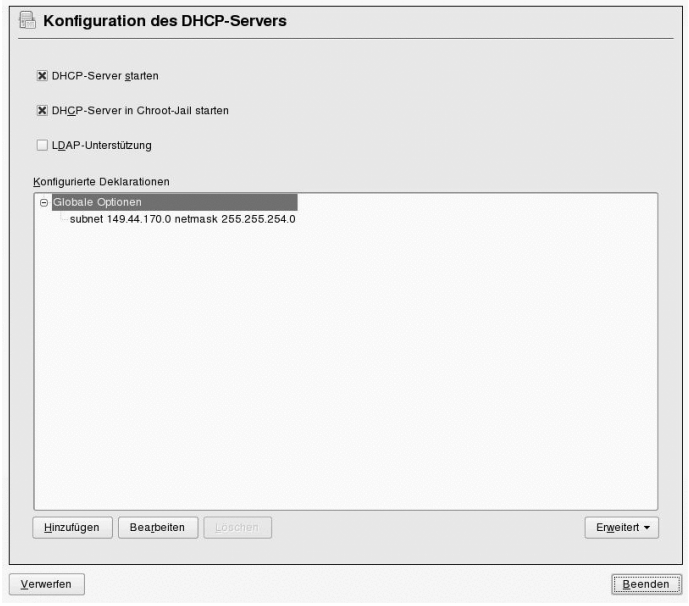


22.1.2 Konfiguration für Experten

Zusätzlich zu den bisher erwähnten Konfigurationsmethoden gibt es einen Expertenkonfigurationsmodus, mit dem Sie die Einrichtung des DHCP-Servers detailgenau ändern können. Starten Sie die Expertenkonfiguration, indem Sie *Einstellungen für Experten* in der Baumstruktur links im Dialogfeld wählen.

Chroot-Umgebung und Deklarationen
: Im ersten Dialogfeld bearbeiten Sie die vorhandene Konfiguration, indem Sie *DHCP-Server starten* wählen. Eine wichtige Funktion des Verhaltens eines DHCP-Servers ist, dass er in einer Chroot-Umgebung (oder einem Chroot-Jail) ausgeführt werden kann und so den Server-Host schützt. Sollte der DHCP-Server durch einen Angriff von außen beeinträchtigt werden, bleibt der Angreifer gefangen im Chroot-Jail und kann auf den Rest des Systems nicht zugreifen. Im unteren Bereich des Dialogfelds sehen Sie eine Baumstruktur mit den bereits definierten Deklarationen. Diese verändern Sie mit *Hinzufügen*, *Löschen* und *Bearbeiten*. Wenn Sie *Erweitert* wählen, werden zusätzliche Experten-Dialogfelder angezeigt. Weitere Informationen hierzu finden Sie unter Abbildung 22.6, „DHCP-Server: Chroot Jail und Deklarationen“ (S. 348). Nach der Auswahl von *Hinzufügen* legen Sie den hinzuzufügenden Deklarationstyp fest. Mit *Erweitert* zeigen Sie die Protokolldatei des Servers an, konfigurieren die TSIG-Schlüsselverwaltung und passen die Konfiguration der Firewall an die Einrichtung des DHCP-Servers an.

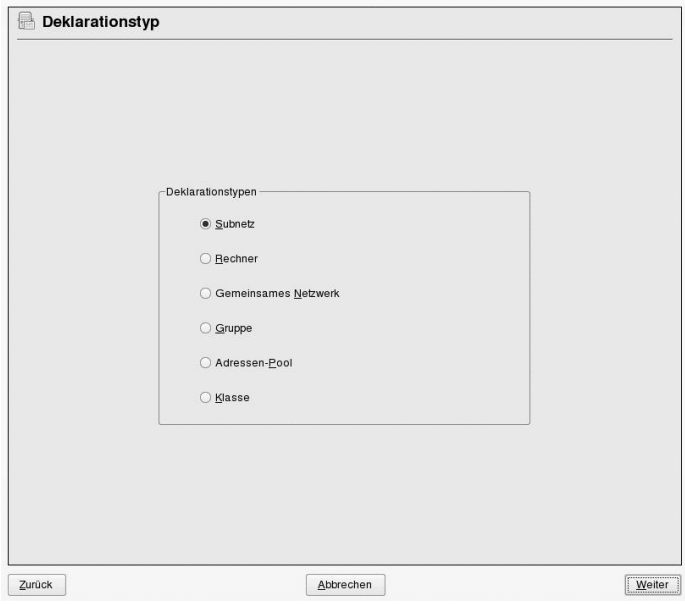
Abbildung 22.6 *DHCP-Server: Chroot Jail und Deklarationen*



Auswählen des Deklarationstyps

Die *Globalen Optionen* des DHCP-Servers bestehen aus einer Reihe von Deklarationen. In diesem Dialogfeld legen Sie die Deklarationstypen *Subnetz*, *Host*, *Gemeinsames Netzwerk*, *Gruppe*, *Adressen-Pool* und *Klasse* fest. In diesem Beispiel sehen Sie die Auswahl eines neuen Subnetzwerks (siehe Abbildung 22.7, „DHCP-Server: Wählen eines Deklarationstyps“ (S. 349)).

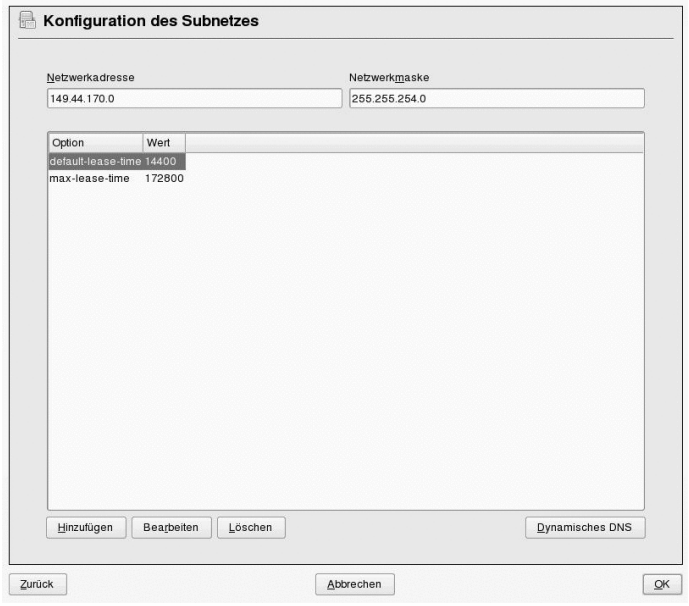
Abbildung 22.7 *DHCP-Server: Wählen eines Deklarationstyps*



Konfiguration des Subnetzes

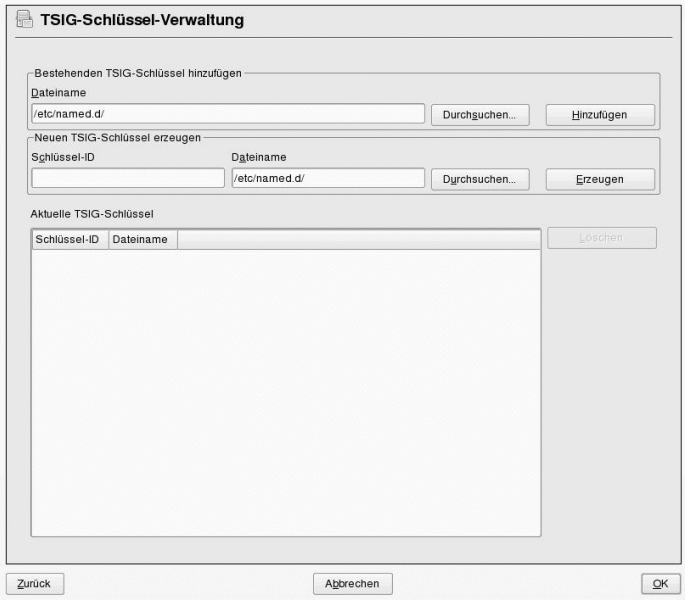
In diesem Dialogfeld können Sie ein neues Subnetz mit seiner IP-Adresse und Netzmaske angeben. In der Mitte des Dialogfelds ändern Sie die Startoptionen des DHCP-Servers für das ausgewählte Subnetz mit den Optionen *Hinzufügen*, *Bearbeiten* und *Löschen*. Um einen dynamischen DNS für das Subnetz einzurichten, wählen Sie *Dynamisches DNS*.

Abbildung 22.8 *DHCP-Server: Konfigurieren von Subnetzen*



TSIG-Schlüsselverwaltung
: Wenn Sie im vorigen Dialogfeld die Konfiguration des dynamischen DNS vorgenommen haben, können Sie jetzt die Schlüsselverwaltung für einen sicheren Zonentransfer konfigurieren. Wenn Sie *OK* wählen, gelangen Sie zu einem weiteren Dialogfeld, in dem Sie die Schnittstelle für das dynamische DNS konfigurieren können (siehe Abbildung 22.10, „DHCP-Server: Schnittstellenkonfiguration für dynamisches DNS“ (S. 352)).

Abbildung 22.9 *DHCP Server: TSIG-Konfiguration*



Dynamisches DNS: Schnittstellenkonfiguration

Jetzt können Sie das dynamische DNS für das Subnetz aktivieren, indem Sie *Dynamisches DNS für dieses Subnetz aktivieren* wählen. Danach wählen Sie in der Dropdown-Liste die TSIG-Schlüssel für Forward und Reverse Zones. Vergewissern Sie sich dabei, dass die Schlüssel für den DNS- und den DHCP-Server dieselben sind. Mit der Option *Globale dynamische DNS-Einstellungen aktualisieren* aktivieren Sie die automatische Aktualisierung und Einstellung der globalen DHCP-Servereinstellungen entsprechend der dynamischen DNS-Umgebung. Nun legen Sie fest, welche Forward und Reverse Zones über das dynamische DNS aktualisiert werden sollen. Dafür geben Sie den primären Namenserver für beide Zonen an. Wenn der Namenserver auf demselben Host wie der DHCP-Server ausgeführt wird, können Sie diese Felder leer lassen. Wenn Sie *OK* wählen, gelangen Sie wieder zum Dialogfeld für die Subnetzkonfiguration (siehe Abbildung 22.8, „DHCP-Server: Konfigurieren von Subnetzen“ (S. 350)). Wenn Sie noch einmal auf *OK* klicken, gelangen Sie wieder zum ursprünglichen Dialogfeld für die Expertenkonfiguration.

Abbildung 22.10 *DHCP-Server: Schnittstellenkonfiguration für dynamisches DNS*

Netzwerkschnittstellenkonfiguration

Wenn Sie die Schnittstellen festlegen möchten, die vom DHCP-Server überwacht werden sollen, und die Firewall-Konfiguration anpassen, wählen Sie im Dialogfeld für die Expertenkonfiguration *Erweitert > Schnittstellenkonfiguration*. Aus der Liste der angezeigten Schnittstellen wählen Sie die gewünschte(n) Schnittstelle(n) für den DHCP-Server aus. Falls Clients in allen Subnetzen mit dem Server kommunizieren sollen und der Server-Host eine Firewall ausführt, passen Sie die Einstellungen der Firewall entsprechend an. Dafür wählen Sie *Firewall-Einstellungen anpassen*. YaST passt dann die Regeln der SuSEfirewall2 an die neuen Bedingungen an (siehe Abbildung 22.11, „DHCP-Server: Netzwerkschnittstelle und Firewall“ (S. 353)). Jetzt können Sie zum ursprünglichen Dialogfeld zurückkehren, indem Sie auf *OK* klicken.

Abbildung 22.11 *DHCP-Server: Netzwerkschnittstelle und Firewall*

Nach Abschluss aller Konfigurationsschritte schließen Sie das Dialogfeld mit *OK*. Der Server wird jetzt mit seiner neuen Konfiguration gestartet.

22.2 DHCP-Softwarepakete

Für SUSE Linux Enterprise Server stehen sowohl ein DHCP-Server als auch DHCP-Clients bereit. Der vom Internet Systems Consortium (ISC) herausgegebene DHCP-Server dhcpd stellt die Serverfunktionalität zur Verfügung. Wählen Sie auf der Client-Seite zwischen zwei verschiedenen DHCP-Client-Programmen: `DHCP-Client` (auch von ISC) und DHCP-Client-Daemon im Paket `dhcpcd`.

SUSE Linux Enterprise Server installiert standardmäßig dhcpcd. Das Programm ist sehr einfach in der Handhabung und wird beim Booten des Computers automatisch gestartet, um nach einem DHCP-Server zu suchen. Es kommt ohne eine Konfigurationsdatei aus und funktioniert im Normalfall ohne weitere Konfiguration. Verwenden Sie für komplexere Situationen das Programm dhcp-client von ISC, das sich über die Konfigurationsdatei `/etc/dhclient.conf` steuern lässt.

22.3 Der DHCP-Server dhcpd

Das Kernstück des DHCP-Systems ist der dhcpd-Daemon. Dieser Server *least* Adressen und überwacht deren Nutzung gemäß den Vorgaben in der Konfigurationsdatei `/etc/dhcpd.conf`. Über die dort definierten Parameter und Werte stehen dem Systemadministrator eine Vielzahl von Möglichkeiten zur Verfügung, das Verhalten des Programms anforderungsgemäß zu beeinflussen. Sehen Sie sich die einfache Beispieldatei `/etc/dhcpd.conf` in Beispiel 22.1, „Die Konfigurationsdatei "/etc/dhcpd.conf"“ (S. 354) an.

Beispiel 22.1 *Die Konfigurationsdatei "/etc/dhcpd.conf"*

```
default-lease-time 600;         # 10 minutes
max-lease-time 7200;            # 2  hours

option domain-name "example.com";
option domain-name-servers 192.168.1.116;
option broadcast-address 192.168.2.255;
option routers 192.168.2.1;
option subnet-mask 255.255.255.0;

subnet 192.168.2.0 netmask 255.255.255.0
 {
  range 192.168.2.10 192.168.2.20;
  range 192.168.2.100 192.168.2.200;
 }
```

Diese einfache Konfigurationsdatei reicht bereits aus, damit der DHCP-Server im Netzwerk IP-Adressen zuweisen kann. Bitte achten Sie insbesondere auf die Semikolons am Ende jeder Zeile, ohne die dhcpd nicht startet.

Die Beispieldatei lässt sich in drei Abschnitte unterteilen. Im ersten Abschnitt wird definiert, wie viele Sekunden eine IP-Adresse standardmäßig an einen anfragenden Client geleast wird, bevor dieser eine Verlängerung anfordern sollte (`default-lease-time`). Hier wird auch festgelegt, wie lange ein Computer maximal eine vom DHCP-Server vergebene IP-Adresse behalten darf, ohne für diese eine Verlängerung anfordern zu müssen (`max-lease-time`).

Im zweiten Abschnitt werden einige grundsätzliche Netzwerkparameter global festgelegt:

- Die Zeile `option domain-name` enthält die Standarddomäne des Netzwerks.

- Mit dem Eintrag `option domain-name-servers` können Sie bis zu drei Werte für die DNS-Server angeben, die zur Auflösung von IP-Adressen in Hostnamen (und umgekehrt) verwendet werden sollen. Idealerweise sollten Sie vor dem Einrichten von DHCP einen Namenserver auf dem Computer oder im Netzwerk konfigurieren. Dieser Namenserver sollte für jede dynamische Adresse jeweils einen Hostnamen und umgekehrt bereithalten. Weitere Informationen zum Konfigurieren eines eigenen Namenservers finden Sie in Kapitel 21, *Domain Name System (DNS)* (S. 313).

- Die Zeile `option broadcast-address` definiert die Broadcast-Adresse, die der anfragende Client verwenden soll.

- Mit `option routers` wird festgelegt, wohin der Server Datenpakete schicken soll, die (aufgrund der Adresse von Quell- und Zielhost sowie der Subnetzmaske) nicht im lokalen Netzwerk zugestellt werden können. Gerade bei kleineren Netzwerken ist dieser Router auch meist mit dem Internet-Gateway identisch.

- Mit `option subnet-mask` wird die den Clients zugewiesene Netzmaske angegeben.

Im letzten Abschnitt der Datei werden ein Netzwerk und eine Subnetzmaske angegeben. Abschließend muss noch ein Adressbereich gewählt werden, aus dem der DHCP-Daemon IP-Adressen an anfragende Clients vergeben darf. In Beispiel 22.1, „Die Konfigurationsdatei "/etc/dhcpd.conf"“ (S. 354) können Clients Adressen zwischen `192.168.2.10` und `192.168.2.20` sowie `192.168.2.100` und `192.168.2.200` zugewiesen werden.

Nachdem Sie diese wenigen Zeilen bearbeitet haben, können Sie den DHCP-Daemon bereits mit dem Befehl `rcdhcpd start` aktivieren. Der DHCP-Daemon ist sofort einsatzbereit. Mit dem Befehl `rcdhcpd check-syntax` können Sie eine kurze Überprüfung der Konfigurationsdatei vornehmen. Wenn ein unerwartetes Problem mit der Konfiguration auftritt (der Server wird mit einem Fehler abgebrochen oder gibt beim Starten nicht `done` zurück), lesen Sie die Informationen in der zentralen Systemprotokolldatei `/var/log/messages` oder auf der Konsole 10 (Strg + Alt + F10).

Auf einem SUSE Linux Enterprise Server-Standardsystem wird der DHCP-Daemon aus Sicherheitsgründen in einer chroot-Umgebung gestartet. Damit der Daemon die Konfigurationsdateien finden kann, müssen diese in die chroot-Umgebung kopiert

werden. In der Regel müssen Sie dazu nur den Befehl `rcdhcpd start` eingeben, um die Dateien automatisch zu kopieren.

22.3.1 Clients mit statischen IP-Adressen

DHCP lässt sich auch verwenden, um einem bestimmten Client eine vordefinierte statische Adresse zuzuweisen. Solche expliziten Adresszuweisungen haben Vorrang vor dynamischen Adressen aus dem Pool. Im Unterschied zu den dynamischen verfallen die statischen Adressinformationen nie, z. B. wenn nicht mehr genügend freie Adressen zur Verfügung stehen und deshalb eine Neuverteilung unter den Clients erforderlich ist.

Zur Identifizierung eines mit einer statischen Adresse konfigurierten Clients verwendet dhcpd die Hardware-Adresse. Dies ist eine global eindeutige, fest definierte Zahl aus sechs Oktettpaaren, über die jedes Netzwerkgerät verfügt, z. B. `00:30:6E:08:EC:80`. Werden die entsprechenden Zeilen, wie z. B. in Beispiel 22.2, „Ergänzungen zur Konfigurationsdatei“ (S. 356) zur Konfigurationsdatei von Beispiel 22.1, „Die Konfigurationsdatei "/etc/dhcpd.conf"“ (S. 354) hinzugefügt, weist der DHCP-Daemon dem entsprechenden Client immer dieselben Daten zu.

Beispiel 22.2 *Ergänzungen zur Konfigurationsdatei*

```
host jupiter {
hardware ethernet 00:30:6E:08:EC:80;
fixed-address 192.168.2.100;
}
```

Der Name des entsprechenden Clients (`host` *`Hostname`*, hier `jupiter`) wird in die erste Zeile, und die MAC-Adresse wird in die zweite Zeile eingegeben. Auf Linux-Hosts kann die MAC-Adresse mit dem Befehl `iplink show` gefolgt vom Netzwerkgerät (z. B. `eth0`) ermittelt werden. Die Ausgabe sollte in etwa wie folgt aussehen:

```
link/ether 00:30:6E:08:EC:80
```

Im vorherigen Beispiel wird also dem Client, dessen Netzwerkkarte die MAC-Adresse `00:30:6E:08:EC:80` hat, automatisch die IP-Adresse `192.168.2.100` und der Hostname `jupiter` zugewiesen. Als Hardwaretyp kommt heutzutage in aller Regel `ethernet` zum Einsatz, wobei durchaus auch das vor allem bei IBM-Systemen häufig zu findende `token-ring` unterstützt wird.

22.3.2 Die SUSE Linux Enterprise Server-Version

Aus Sicherheitsgründen enthält bei der SUSE Linux Enterprise Server-Version der DHCP-Server von ISC den non-root/chroot-Patch von Ari Edelkind. Damit kann dhcpd mit der Benutzer-ID `nobody` und in einer chroot-Umgebung (`/var/lib/dhcp`) ausgeführt werden. Um dies zu ermöglichen, muss sich die Konfigurationsdatei `dhcpd.conf` im Verzeichnis `/var/lib/dhcp/etc` befinden. Sie wird vom Init-Skript beim Start automatisch dorthin kopiert.

Dieses Verhalten lässt sich über Einträge in der Datei `/etc/sysconfig/dhcpd` steuern. Um den dhcpd ohne chroot-Umgebung laufen zu lassen, setzen Sie die Variable `DHCPD_RUN_CHROOTED` in der Datei `/etc/sysconfig/dhcpd` auf "no".

Damit der dhcpd auch in der chroot-Umgebung Hostnamen auflösen kann, müssen außerdem einige weitere Konfigurationsdateien kopiert werden:

- `/etc/localtime`
- `/etc/host.conf`
- `/etc/hosts`
- `/etc/resolv.conf`

Diese Dateien werden beim Starten des Init-Skripts in das Verzeichnis `/var/lib/dhcp/etc/` kopiert. Berüchsichtigen Sie die Kopien bei Aktualisierungen, die benötigt werden, wenn sie durch ein Skript wie `/etc/ppp/ip-up` dynamisch modifiziert werden. Falls in der Konfigurationsdatei anstelle von Hostnamen nur IP-Adressen verwendet werden, sind jedoch keine Probleme zu erwarten.

Wenn in Ihrer Konfiguration weitere Dateien in die chroot-Umgebung kopiert werden müssen, können Sie diese mit der Variablen `DHCPD_CONF_INCLUDE_FILES` in der Datei `/etc/sysconfig/dhcpd` festlegen. Damit der dhcp-Daemon aus der chroot-Umgebung heraus auch nach einem Neustart des Syslog-ng-Daemons weiter protokollieren kann, befindet sich der zusätzliche Eintrag `SYSLOGD_ADDITIONAL_SOCKET_DHCP` in der Datei `/etc/sysconfig/syslog`.

22.4 Weiterführende Informationen

Weitere Informationen zu DHCP finden Sie auf der Website des *Internet Systems Consortium* (`http://www.isc.org/products/DHCP/`). Weitere Informationen finden Sie zudem auf den man-Seiten `dhcpd`, `dhcpd.conf`, `dhcpd.leases` und `dhcp-options`.

Verwenden von NetworkManager

23

NetworkManager ist die ideale Lösung für Notebooks und andere portable Computer. Wenn Sie viel unterwegs sind und NetworkManager verwenden, brauchen Sie keine Gedanken mehr an die Konfiguration von Netzwerkschnittstellen und den Wechsel zwischen verkabelten und drahtlosen Netzwerken zu verschwenden. NetworkManager kann die Verbindung mit bekannten drahtlosen Netzwerken automatisch herstellen. Es kann auch verschiedene Netzwerkverbindungen parallel verwalten; in diesem Fall wird standardmäßig die schnellste Verbindung verwendet. Zudem können Sie manuell zwischen den verfügbaren Netzwerken wechseln und Ihre Netzwerkverbindung über ein Miniprogramm (Applet oder Widget) im Systemabschnitt der Kontrollleiste verwalten.

Auf Laptop-Computern ist NetworkManager standardmäßig aktiv. Es kann jedoch jederzeit mit YaST aktiviert oder deaktiviert werden, wie in Abschnitt 23.2, „Aktivieren von NetworkManager“ (S. 360) beschrieben.

23.1 Anwendungsbeispiele für NetworkManager

NetworkManager stellt eine ausgereifte und intuitive Benutzerschnittstelle bereit, über die die Benutzer mühelos den Wechsel zwischen Netzwerkumgebungen vornehmen können. In folgenden Fällen ist NetworkManager jedoch ungeeignet:

- Ihr Computer stellt Netzwerkdienste für andere Computer in Ihrem Netzwerk bereit (es handelt sich zum Beispiel um einen DHCP- oder DNS-Server)

- Ihr Computer ist ein Xen-Server oder Ihr System ein virtuelles System innerhalb von Xen.
- Sie möchten SCPM verwenden, um die Netzwerkkonfiguration zu verwalten Möchten Sie SCPM und den NetworkManager zur gleichen Zeit verwenden, müssen Sie die Netzwerkressource in der SCPM-Konfiguration deaktivieren.

23.2 Aktivieren von NetworkManager

Wenn Sie Ihre Netzwerkverbindung mit NetworkManager verwalten möchten, aktivieren Sie NetworkManager im Modul 'Netzwerkeinstellungen' von YaST. Gehen Sie zur Aktivierung von NetworkManager folgendermaßen vor:

1. Starten Sie YaST und gehen Sie zu *Netzwerkgeräte* > *Netzwerkeinstellungen*.
2. Das Dialogfeld *Netzwerkeinstellungen* wird geöffnet. Klicken Sie auf den Karteireiter *Globale Optionen*.
3. Aktivieren Sie im Feld *Netzwerkeinrichtungsmethode* die Option *Benutzergesteuert mithilfe von NetworkManager*.
4. Klicken Sie auf *Fertig stellen*.
5. Nach Auswahl der Methode zur Verwaltung von Netzwerkverbindungen richten Sie Ihre Netzwerkkarte mithilfe der automatischen Konfiguration über DHCP oder eine statische IP-Adresse ein oder konfigurieren Sie Ihr Modem (für Einwahlverbindungen verwenden Sie *Netzwerkgeräte* > *Modem*). Wählen Sie *Netzwerkgeräte* > *ISDN*, um ein internes ISDN-Modem oder ein USB-ISDN-Modem zu konfigurieren. Wählen Sie *Netzwerkgeräte* > *DSL*, um ein internes DSL-Modem oder ein USB-DSL-Modem zu konfigurieren.

   Eine ausführliche Beschreibung der Netzwerkkonfiguration mit YaST erhalten Sie unter Abschnitt 17.4, „Konfigurieren von Netzwerkverbindungen mit YaST“ (S. 240) und Abschnitt 18.1, „Wireless LAN“ (S. 287).

Nach der Aktivierung von NetworkManager können Sie Ihre Netzwerkverbindungen mit NetworkManager konfigurieren, wie unter Abschnitt 23.3, „Konfigurieren von Netzwerkverbindungen“ (S. 361) beschrieben.

Wenn Sie NetworkManager deaktivieren und das Netzwerk auf die herkömmliche Weise steuern möchten, wählen Sie im Feld *Netzwerkeinrichtungsmethode* die Option *Traditionelle Methode mit ifup*.

23.3 Konfigurieren von Netzwerkverbindungen

Nach der Aktivierung von NetworkManager in YaST können Sie Ihre Netzwerkverbindungen über das GNOME-Kontrollzentrum oder über die persönlichen Einstellungen von KDE 4 in einem Dialogfeld konfigurieren. Wenn Sie GNOME verwenden, starten Sie das GNOME-Kontrollzentrum aus dem Hauptmenü und wählen Sie dort *System > Netzwerkkonfigurationen* aus, um das Dialogfeld *Netzwerkkonfiguration* zu öffnen. Wenn Sie KDE verwenden, klicken Sie im Hauptmenü auf *Desktop konfigurieren*, um *Persönliche Einstellungen* zu öffnen und wählen Sie dann *Erweitert > Netzwerkeinstellungen* aus, um das Dialogfeld *Netzwerkeinstellungen* zu öffnen.

Abbildung 23.1 *Dialogfeld 'Netzwerkkonfiguration' von GNOME*

Die Konfigurationsdialogfelder können alternativ auch über das Miniprogramm NetworkManager im Systemabschnitt der Kontrollleiste geöffnet werden. Klicken Sie dort auf *Konfigurieren* (KDE) oder klicken Sie mit der rechten Maustaste auf das GNOME-Miniprogramm und wählen Sie *Verbindungen bearbeiten* aus.

Die Konfigurationsdialogfelder von GNOME und KDE 4 enthalten für jeden Netzwerkverbindungstyp Karteireiter (z. B. Kabelverbindungen, drahtlose Verbindungen, Mobile Broadband-Verbindungen sowie DSL- und VPN-Verbindungen). NetworkManager unterstützt auch Verbindungen mit geschützten 802.1X-Netzwerken.

Zum Hinzufügen einer neuen Verbindung klicken Sie auf den Karteireiter für die zu verwendende Verbindungsart und klicken Sie auf *Hinzufügen*. Geben Sie einen *Verbindungsnamen* und Ihre Verbindungsdetails ein. Wenn mehrere physische Geräte pro Verbindungstyp verfügbar sind (z. B. wenn Ihr Computer mit zwei Ethernet-Karten oder zwei Wireless-Karten ausgestattet ist), geben Sie die *MAC-Adresse* (die Hardware-Adresse) des Geräts an, um die Verbindung an dieses Gerät zu binden. Klicken Sie auf *OK* oder *Anwenden*, um Ihre Einstellungen zu bestätigen. Die neu konfigurierte Netzwerkverbindung wird nun in der Liste der verfügbaren Netzwerke angezeigt, die durch Klicken mit der rechten Maustaste auf das Miniprogramm NetworkManager geöffnet wird.

ANMERKUNG: Verborgene Netzwerke

Um eine Verbindung zu einem "verborgenen" Netzwerk aufzubauen (einem Netzwerk, das seinen Dienst nicht als Broadcast ausführt), müssen Sie den Extended Service Set Identifier (ESSID) des Netzwerks kennen, da er nicht automatisch erkannt wird. Geben Sie in diesem Fall die ESSID und bei Bedarf auch die Verschlüsselungsparameter ein.

Beim Einrichten der einzelnen Verbindungen können Sie auch festlegen, ob NetworkManager die jeweilige Verbindung automatisch (aktivieren Sie *Connect Automatically* (Automatisch verbinden)) oder systemweit (aktivieren Sie *Available to all users* (Für alle Benutzer verfügbar)) verwenden soll. Solche Systemverbindungen können alle Benutzer freigeben und direkt nach dem Start von NetworkManager zur Verfügung stellen, bevor sich Benutzer angemeldet haben. Zum Erstellen und Bearbeiten von Systemverbindungen ist die `root`-Berechtigung erforderlich.

23.4 Verwenden des KDE-Widgets NetworkManager

In KDE 4 wurde das Miniprogramm KNetworkManager zur Steuerung von NetworkManager durch das Widget NetworkManager ersetzt. Widgets sind kleine Anwendungen,

die in Ihren Desktop oder Ihre Kontrollleiste integriert werden können. Wenn das Netzwerk für die Verwaltung durch NetworkManager eingerichtet ist, wird das Widget normalerweise automatisch mit der Desktop-Umgebung gestartet und im Systemabschnitt der Kontrollleiste als Symbol angezeigt.

Das NetworkManager-Widget zeigt den aktuellen Netzwerkstatus als Symbol an und meldet Änderungen mittels Benachrichtigungen. Mit dem Widget können Sie neue Netzwerkverbindungen konfigurieren, manuell eine andere Netzwerkverbindung auswählen, die Verwendung drahtloser Netzwerke deaktivieren oder auch ganz in den Offline-Modus wechseln. Das Aussehen des Symbols hängt vom Typ und Status der aktuellen Netzwerkverbindung ab. Wenn Sie den Mauszeiger auf das Symbol verschieben, werden Details zur Verbindung angezeigt.

NetworkManager unterscheidet zwei Arten von Verbindungen: verbürgte und unverbürgte Verbindungen. Eine verbürgte Verbindung ist jedes Netzwerk, das Sie explizit ausgewählt haben. Alle anderen sind unverbürgt. Klicken Sie mit der rechten Maustaste auf die Verbindungssymbole, um eine Liste der Verbindungen anzuzeigen, die Sie in der Vergangenheit mindestens einmal verwendet haben. Die derzeit verwendete Verbindung ist im Menü gekennzeichnet.

Klicken Sie mit der linken Maustaste auf eines der Verbindungs-Miniprogramme, um zu einem beliebigen Zeitpunkt eine andere Netzwerkverbindung zu wählen. Diese Auswahl hat Vorrang vor automatisch ausgewählten Netzwerken. Das ausgewählte Netzwerk wird so lange verwendet, wie es verfügbar ist. Dies bedeutet, dass die Verbindung beim Einstecken eines Netzwerkkabels nicht automatisch auf die verkabelte Netzwerkverbindung umgeschaltet wird.

23.5 Verwendung des GNOME NetworkManager-Miniprogramms

In GNOME kann NetworkManager mithilfe des GNOME NetworkManager-Miniprogramms gesteuert werden. Wenn das Netzwerk zur NetworkManager-Steuerung eingerichtet ist, startet das Miniprogramm normalerweise automatisch mit der Desktop-Umgebung und wird im Systemabschnitt der Kontrollleiste als Symbol angezeigt.

Wenn das GNOME NetworkManager-Miniprogramm im Systemabschnitt der Kontrollleiste nicht angezeigt wird, wurde das Miniprogramm wahrscheinlich nicht gestartet. Drücken Sie Alt + F2 und geben Sie `nm-applet` ein, um es manuell zu starten.

23.5.1 Verbinden mit Kabelnetzwerken

Wenn Ihr Computer mit einem vorhanden Netzwerk über Netzwerkkabel verbunden ist, verwenden Sie das NetworkManager-Miniprogramm zur Auswahl der Netzwerkverbindung.

1. Klicken Sie mit der linken Maustaste auf das Applet-Symbol, um ein Menü mit verfügbaren Netzwerken anzuzeigen. Die zurzeit verwendete Verbindung ist im Menü ausgewählt.

2. Um zu einem anderen Netzwerk zu wechseln, wählen Sie es in der Liste aus.

3. Klicken Sie zum Ausschalten aller Netzwerkverbindungen, sowohl der Kabelverbindungen als auch der drahtlosen Verbindungen, mit der rechten Maustaste auf das Symbol des Miniprogramms und deaktivieren Sie das Kontrollkästchen für *Netzwerk aktivieren*.

23.5.2 Verbinden mit drahtlosen Netzwerken

Verfügbare sichtbare drahtlose Netzwerke werden im Menü des GNOME NetworkManager-Miniprogramms unter *Drahtlose Netzwerke* aufgeführt. Die Signalstärke der einzelnen Netzwerke wird ebenfalls im Menü angezeigt. Verschlüsselte drahtlose Netzwerke sind mit einem blauen Schildsymbol gekennzeichnet.

Prozedur 23.1 *Verbinden mit einem drahtlosen Netzwerk*

1. Klicken Sie zum Verbinden mit einem drahtlosen Netzwerk mit der linken Maustaste auf das Symbol für das Miniprogramm und wählen Sie einen Eintrag aus der Liste der verfügbaren drahtlosen Netzwerke aus.

2. Wenn das Netzwerk verschlüsselt ist, öffnet sich ein Dialogfeld. Wählen Sie die Art der *Sicherheit des drahtlosen Netzwerks*, die das Netzwerk verwendet, und geben Sie das entsprechende *Passwort* ein.

3. Um eine Verbindung mit einem Netzwerk herzustellen, das seinen ESSID (Service Set Identifier) nicht sendet und demzufolge nicht automatisch erkannt werden

kann, klicken Sie mit der linken Maustaste auf das NetworkManager-Symbol und wählen Sie *Verbindung zu anderem drahtlosen Netzwerk herstellen*.

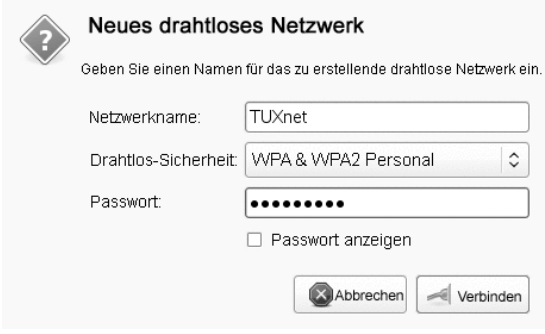
4 Geben Sie in dem daraufhin angezeigten Dialogfeld den ESSID ein und legen Sie gegebenenfalls die Verschlüsselungsparameter fest.

5 Um drahtlose Netzwerkverbindungen zu deaktivieren, klicken Sie mit der rechten Maustaste auf das Applet-Symbol und deaktivieren Sie die Option *Drahtlose Netzwerke aktivieren*. Dies kann sehr nützlich sein, wenn Sie sich in einem Flugzeug befinden oder in einer anderen Umgebung, in der drahtlose Netzwerke nicht zulässig sind.

23.5.3 Konfigurieren der drahtlosen Netzwerkkarte als Zugriffspunkt

Wenn Ihre drahtlose Netzwerkkarte den Zugriffspunktmodus unterstützt, können Sie den NetworkManager für die Konfiguration verwenden.

1 Klicken Sie auf *Neues drahtloses Netzwerk erstellen*.



2 Fügen Sie den Netzwerknamen hinzu und legen Sie im Dialogfeld *Drahtlose Sicherheit* die Verschlüsselung fest.

WICHTIG: Ungeschützte drahtlose Netzwerke stellen ein Sicherheitsrisiko dar

Wenn Sie *Drahtlose Sicherheit* auf `None` (Keine) einstellen, kann jeder eine Verbindung zu Ihrem Netzwerk herstellen, Ihre Verbindung verwenden und Ihre Netzwerkverbindung abfangen. Verwenden Sie die Verschlüsselung, um den Zugriff auf Ihren Zugriffspunkt zu beschränken und Ihre Verbindung zu schützen. Sie können zwischen verschiedenen WEP-(Wired Equivalent Privacy-) und auf WPA (Wi-Fi Protected Access) basierten Verschlüsselungen wählen. Wenn Sie sich nicht sicher sind, welche Technologie für Sie am besten geeignet ist, lesen Sie „Authentifizierung“ (S. 289).

23.6 NetworkManager und VPN

NetworkManager unterstützt verschiedene Technologien für virtuelle private Netzwerke (VPN):

- NovellVPN—package `NetworkManager-novellvpn`
- OpenVPN—package `NetworkManager-openvpn`
- vpnc (Cisco)—package `NetworkManager-vpnc`
- PPTP (Point-to-Point Tunneling Protocol) – Paket `NetworkManager-pptp`

Zur Verwendung von VPN mit NetworkManager installieren Sie zunächst die entsprechenden VPN-Pakete. Sie benötigen zwei Pakete für jede VPN-Technologie: Eines der oben genannten Pakete (mit generischer Unterstützung für NetworkManager) sowie das entsprechende desktopspezifische Paket für Ihr Miniprogramm.

Wählen Sie für KDE eines der folgenden Pakete aus:

- NovellVPN-Unterstützung für KNetworkManager – Paket `NetworkManager-novellvpn-kde`
- OpenVPN-Unterstützung für KNetworkManager – Paket `NetworkManager-openvpn-kde4`

- vpnc (Cisco)-Unterstützung für KNetworkManager – Paket `NetworkManager-vpnc-kde4`

PPTP-Unterstützung für KDE steht zurzeit noch nicht zur Verfügung, es wird jedoch daran gearbeitet.

Wählen Sie für GNOME eines der folgenden Pakete aus:

- NovellVPN support for GNOME NetworkManager applet—package `NetworkManager-novellvpn-gnome`
- OpenVPN support for GNOME NetworkManager applet—package `NetworkManager-openvpn-gnome`
- vpnc (Cisco) support for GNOME NetworkManager applet—package `NetworkManager-vpnc-gnome`
- PPTP (Point-to-Point Tunneling Protocol)-Unterstützung für das GNOME-Miniprogramm NetworkManager – Paket `NetworkManager-pptp-gnome`

Konfigurieren Sie Ihre VPN-Verbindung nach der Installation der Pakete, wie in Abschnitt 23.3, „Konfigurieren von Netzwerkverbindungen“ (S. 361) beschrieben.

23.7 NetworkManager und Sicherheit

NetworkManager unterscheidet zwei Arten von drahtlosen Verbindungen: verbürgte und unverbürgte Verbindungen. Eine verbürgte Verbindung ist jedes Netzwerk, das Sie in der Vergangenheit explizit ausgewählt haben. Alle anderen sind unverbürgt. Verbürgte Verbindungen werden anhand des Namens und der MAC-Adresse des Zugriffspunkts identifiziert. Durch Verwendung der MAC-Adresse wird sichergestellt, dass Sie keinen anderen Zugriffspunkt mit dem Namen Ihrer verbürgten Verbindung verwenden können.

NetworkManager scannt in regelmäßigen Abständen nach verfügbaren drahtlosen Netzwerken. Wenn mehrere verbürgte Netzwerke gefunden werden, wird automatisch das zuletzt verwendete ausgewählt. Wenn keines der Netzwerke vertrauenswürdig ist, wartet NetworkManager auf Ihre Auswahl.

Wenn die Verschlüsselungseinstellung geändert wird, aber Name und MAC-Adresse gleich bleiben, versucht der NetworkManager, eine Verbindung herzustellen. Zuvor werden Sie jedoch aufgefordert, die neuen Verschlüsselungseinstellungen zu bestätigen und Aktualisierungen, wie z. B. einen neuen Schlüssel, bereitzustellen.

NetworkManager kennt zwei Verbindungsarten: `Benutzer-` und `System-`Verbindungen. Bei Benutzerverbindungen handelt es sich um Verbindungen, die für NetworkManager verfügbar werden, sobald sich der erste Benutzer anmeldet. Alle erforderlichen Legitimationsdaten werden vom Benutzer angefordert, und wenn er sich abmeldet, werden die Verbindungen getrennt und von NetworkManager entfernt. Als Systemverbindung definierte Verbindungen können für alle Benutzer freigegeben werden und sind direkt nach dem Start von NetworkManager verfügbar, bevor sich Benutzer angemeldet haben. Für Systemverbindungen müssen alle Berechtigungsnachweise zum Zeitpunkt der Verbindungserstellung angegeben werden. Über Systemverbindungen können automatisch Verbindungen mit Netzwerken hergestellt werden, für die eine Autorisierung erforderlich ist. Informationen zum Konfigurieren von Benutzer- oder Systemverbindungen finden Sie unter Abschnitt 23.3, „Konfigurieren von Netzwerkverbindungen“ (S. 361).

Wenn Sie nach Verwendung einer drahtlosen Verbindung in den Offline-Modus wechseln, löscht der NetworkManager die ESSID. So wird sichergestellt, dass die Karte nicht mehr verwendet wird.

23.7.1 Speichern von Passwörtern und Berechtigungsnachweisen

Wenn Sie Ihre Berechtigungsnachweise nicht bei jedem Verbindungsversuch mit einem verschlüsselten Netzwerk erneut eingeben wollen, können Sie die Desktop-spezifischen Werkzeuge oder den GNOME Keyring Manager oder KWalletManager verwenden, um Ihre Berechtigungsnachweise verschlüsselt und durch Master-Passwort geschützt auf der Festplatte zu speichern.

NetworkManager kann auch seine Zertifikate für sichere Verbindungen (z. B. verschlüsselte Kabel-, Funk- oder VPN-Verbindungen) vom Zertifikatspeicher abrufen. Weitere Informationen hierzu finden Sie in Kapitel 13, *Certificate Store* (↑*Security Guide*).

23.8 Häufig gestellte Fragen

Nachfolgend finden Sie einige häufig gestellte Fragen zum Konfigurieren spezieller Netzwerkoptionen mit NetworkManager.

Wie kann eine Verbindung an ein bestimmtes Gerät gebunden werden?

Standardmäßig sind Verbindungen in NetworkManager Gerätetyp-spezifisch: Sie gelten für alle physischen Geräte desselben Typs. Wenn mehrere physische Geräte pro Verbindungstyp verfügbar sind (z. B. wenn Ihr Computer mit zwei Ethernet-Karten ausgestattet ist), können Sie eine Verbindung an ein bestimmtes Gerät knüpfen, indem Sie explizit dessen Hardwareadresse (oder MAC-Adresse) angeben.

Schlagen Sie die MAC-Adresse Ihres Geräts in der *Verbindungsinformation* nach, die über das Applet/Widget zur Verfügung steht, oder verwenden Sie die Ausgabe von Kommandozeilenwerkzeugen wie `nm-tool` oder `ifconfig`. Starten Sie dann den Dialog zum Konfigurieren von Netzwerkverbindungen im GNOME-Kontrollzentrum mit *System > Netzwerkkonfigurationen* oder in KDE 4 unter *Persönliche Einstellungen* mit *Erweitert > Netzwerkeinstellungen*. Wählen Sie die Verbindung, die Sie ändern möchten, und klicken Sie auf *Bearbeiten*. Geben Sie im Karteireiter *Verkabelt* oder *Drahtlos* die *MAC-Adresse* des Geräts ein und bestätigen Sie Ihre Änderungen mit *OK*.

Wie wird ein bestimmter Zugriffspunkt angegeben, wenn mehrere Zugriffspunkte mit derselben ESSID erkannt werden?

Wenn mehrere Zugriffspunkte mit unterschiedlichen Funkfrequenzbereichen (a/b/g/n) verfügbar sind, wird standardmäßig der Zugriffspunkt mit dem stärksten Signal automatisch gewählt. Um diesen Vorgang außer Kraft zu setzen, verwenden Sie das Feld *BSSID* beim Konfigurieren Ihrer drahtlosen Verbindungen.

Der Basic Service Set Identifier (BSSID) identifiziert jedes Basic Service Set eindeutig. In einem Basic Service Set der Infrastruktur entspricht die BSSID der MAC-Adresse des drahtlosen Zugriffspunkts. In einem unabhängigen (Ad-hoc) Basic Service Set entspricht die BSSID einer lokal verwalteten MAC-Adresse, die aus einer 46-Bit-Zufallszahl generiert wird.

Starten Sie den Dialog zum Konfigurieren von Netzwerkverbindungen im GNOME-Kontrollzentrum mit *System > Netzwerkkonfigurationen* oder in KDE 4 unter *Persönliche Einstellungen* mit *Erweitert > Netzwerkeinstellungen*. Wählen Sie die

drahtlose Verbindung, die Sie ändern möchten, und klicken Sie auf *Bearbeiten*. Geben Sie im Karteireiter *Drahtlos* die BSSID ein.

Wie werden Netzwerkverbindungen mit anderen Computern freigegeben?

Das primäre Gerät (das Gerät, das mit dem Internet verbunden ist) benötigt keine spezielle Konfiguration. Jedoch müssen Sie das Gerät, das mit dem lokalen Hub oder Computer verbunden ist, wie folgt konfigurieren:

1. Starten Sie den Dialog zum Konfigurieren von Netzwerkverbindungen im GNOME-Kontrollzentrum mit *System > Netzwerkkonfigurationen* oder in KDE 4 unter *Persönliche Einstellungen* mit *Erweitert > Netzwerkeinstellungen*. Wählen Sie die Verbindung, die Sie ändern möchten, und klicken Sie auf *Bearbeiten*. Öffnen Sie den Karteireiter *IPv4-Einstellungen*. Wählen Sie aus der Dropdown-Liste *Methode* die Option *Shared to other computers* (Freigegeben für andere Computer). Damit ist die Weiterleitung von IP-Netzwerkverkehr möglich und ein DHCP-Server wird auf dem Gerät ausgeführt. Bestätigen Sie Ihre Änderungen in NetworkManager.

2. Da der DCHP-Server den Port 67 verwendet, stellen Sie sicher, dass dieser nicht durch die Firewall blockiert ist: Starten Sie YaST auf dem Computer, der die Verbindungen nutzen möchte, und wählen Sie *Sicherheit und Benutzer > Firewall*. Wechseln Sie zur Kategorie *Erlaubte Dienste*. Wenn *DCHP-Server* nicht bereits als *Erlaubter Dienst* angezeigt ist, wählen Sie *DCHP-Server* aus *Services to Allow* (Erlaubte Dienste) und klicken Sie auf *Hinzufügen*. Bestätigen Sie Ihre Änderungen in YaST.

Wie kann statische DNS-Information mit automatischen (DHCP-, PPP-, VPN-) Adressen bereitgestellt werden?

Falls ein DHCP-Server ungültige DNS-Informationen (und/oder Routen) liefert, können Sie diese überschreiben. Starten Sie den Dialog zum Konfigurieren von Netzwerkverbindungen im GNOME-Kontrollzentrum mit *System > Netzwerkkonfigurationen* oder in KDE 4 unter *Persönliche Einstellungen* mit *Erweitert > Netzwerkeinstellungen*. Wählen Sie die Verbindung, die Sie ändern möchten, und klicken Sie auf *Bearbeiten*. Öffnen Sie den Karteireiter *IPv4-Einstellungen* und wählen Sie aus der Dropdown-Liste *Methode* die Option *Automatic (DHCP) addresses only* (Nur automatische (DHCP-) Adressen). Geben Sie die DNS-Information in die Felder *DNS-Server* und *Suchdomänen* ein. Klicken Sie auf *Routen*, um weitere Routen hinzuzufügen oder automatische Routen zu überschreiben. Bestätigen Sie Ihre Änderungen.

Wie kann NetworkManager veranlasst werden, eine Verbindung zu passwortgeschützten Netzwerken aufzubauen, bevor sich ein Benutzer anmeldet?

Definieren Sie eine `Systemverbindung`, die für solche Zwecke verwendet werden kann. Weitere Informationen hierzu finden Sie in Abschnitt 23.7, „NetworkManager und Sicherheit“ (S. 367).

23.9 Fehlersuche

Es können Verbindungsprobleme auftreten. Einige der häufigsten Probleme in Verbindung mit dem NetworkManager sind u. a., dass das Miniprogramm nicht gestartet wird, eine VPN-Option fehlt und Probleme mit SCPM auftreten. Die Methoden zum Lösen und Verhindern dieser Probleme hängen vom verwendeten Werkzeug ab.

Das Desktop-Miniprogramm NetworkManager wird nicht gestartet

Das Miniprogramm NetworkManager von GNOME (Applet) bzw. von KDE (Widget) sollte automatisch gestartet werden, wenn das Netzwerk für die Verwaltung durch NetworkManager eingerichtet ist. Wenn das Miniprogramm nicht gestartet wird, überprüfen Sie, ob NetworkManager in YaST aktiviert ist (siehe Abschnitt 23.2, „Aktivieren von NetworkManager“ (S. 360)). Vergewissern Sie sich danach, ob das richtige Paket für Ihre Desktop-Umgebung installiert ist. Wenn Sie KDE 4 verwenden, muss das Paket `NetworkManager-kde4` installiert sein. Wenn Sie GNOME verwenden, muss das Paket `NetworkManager-gnome` installiert sein.

Wenn das Miniprogramm des GNOME-Desktops installiert ist, aber aus irgendeinem Grund nicht ausgeführt wird (weil Sie es vielleicht unabsichtlich beendet haben), starten Sie es manuell mit dem Kommando `nm-applet`.

Wenn der Systemabschnitt der KDE 4-Kontrollleiste kein Symbol für Netzwerkverbindungen enthält (weil Sie vielleicht in YaST mit NetworkManager von einer statischen zu einer benutzergesteuerten Netzwerkverbindung gewechselt haben), fügen Sie das Widget NetworkManager der Kontrollleiste hinzu. Klicken Sie dazu mit der rechten Maustaste auf einen leeren Bereich der Kontrollleiste und wählen Sie *Panel Options* > *Add Widgets* (Kontrollleistenoptionen, Widgets hinzufügen) aus. (Wenn Ihre Desktop-Objekte zurzeit gesperrt sind, müssen Sie auf *Unlock Widgets* (Widgets entsperren) klicken, um Objekte hinzufügen zu können.) Wählen Sie im daraufhin angezeigten Dialogfeld *NetworkManager* aus und klicken Sie auf *Add Widget* (Widget hinzufügen).

Das Miniprogramm NetworkManager (Applet oder Widget) beinhaltet keine VPN-Option
: Die Unterstützung für NetworkManager-Miniprogramme sowie VPN für NetworkManager wird in Form separater Pakete verteilt. Wenn das Miniprogramm NetworkManager keine VPN-Option enthält, überprüfen Sie, ob die Pakete mit der NetworkManager-Unterstützung für Ihre VPN-Technologie installiert sind. Weitere Informationen finden Sie unter Abschnitt 23.6, „NetworkManager und VPN“ (S. 366).

SCPM schaltet die Netzwerkkonfiguration nicht um
: Wahrscheinlich verwenden Sie SCPM zusammen mit NetworkManager. Der NetworkManager ist zurzeit nicht in der Lage, mit SCPM-Profilen zu arbeiten. Verwenden Sie den NetworkManager nicht gemeinsam mit SCPM, wenn die Netzwerkeinstellungen durch SCPM-Profile geändert werden. Möchten Sie SCPM und den NetworkManager zur gleichen Zeit verwenden, müssen Sie die Netzwerkressource in der SCPM-Konfiguration deaktivieren.

Keine Netzwerkverbindung verfügbar
: Wenn Sie Ihre Netzwerkverbindung korrekt konfiguriert haben und alle anderen Komponenten für die Netzwerkverbindung (Router etc.) auch gestartet sind und ausgeführt werden, ist es manchmal hilfreich, die Netzwerkschnittstellen auf Ihrem Computer erneut zu starten. Melden Sie sich dazu bei einer Kommandozeile als `root` an und führen Sie einen `rcnetwork-Neustart` aus.

23.10 Weiterführende Informationen

Weitere Informationen zu NetworkManager finden Sie auf den folgenden Websites und in den folgenden Verzeichnissen:

- `http://www.gnome.org/projects/NetworkManager/`– Projektseite NetworkManager
- Weitere Informationen zum KDE-Widget NetworkManager finden Sie in `http://userbase.kde.org/KNetworkManager`.
- Sehen Sie sich auch die neuesten Informationen zu NetworkManager und den Miniprogrammen NetworkManager (GNOME-Applet bzw. KDE-Widget) in den folgenden Verzeichnissen an: `/usr/share/doc/packages/NetworkManager/`, `/usr/share/doc/packages/`

`NetworkManager-kde4/` und `/usr/share/doc/packages/NetworkManager-gnome/`

24 Samba

Mit Samba kann ein Unix-Computer als Datei- und Druckserver für Mac OS X-, Windows- und OS/2-Computer konfiguriert werden. Samba ist mittlerweile ein sehr umfassendes und komplexes Produkt. Konfigurieren Sie Samba mit YaST, SWAT (eine Web-Schnittstelle) oder indem Sie die Konfigurationsdatei manuell bearbeiten.

24.1 Terminologie

Im Folgenden werden einige Begriffe erläutert, die in der Samba-Dokumentation und im YaST-Modul verwendet werden.

SMB-Protokoll
: Samba verwendet das SMB-Protokoll (Server Message Block), das auf den NetBIOS-Diensten basiert. Microsoft veröffentlichte das Protokoll, damit auch andere Softwarehersteller Anbindungen an ein Microsoft-Domänennetzwerk einrichten konnten. Samba setzt das SMB- auf das TCP/IP-Protokoll auf. Entsprechend muss auf allen Clients das TCP/IP-Protokoll installiert sein.

TIPP: IBM-System z: NetBIOS-Unterstützung

IBM-System z unterstützen nur SMB über TCP/IP. NetBIOS-Unterstützung ist auf diesen Systemen nicht verfügbar.

CIFS-Protokoll
: Das CIFS-Protokoll (Common Internet File System) ist ein weiteres von Samba unterstütztes Protokoll. CIFS definiert ein Standardprotokoll für den Fernzugriff

auf Dateisysteme über das Netzwerk, das Benutzergruppen die netzwerkweite Zusammenarbeit und gemeinsame Dokumentbenutzung ermöglicht.

NetBIOS
: NetBIOS ist eine Softwareschnittstelle (API) für die Kommunikation zwischen Computern, die einen Name Service bereitstellen. Mit diesem Dienst können die an das Netzwerk angeschlossenen Computer Namen für sich reservieren. Nach dieser Reservierung können die Computer anhand ihrer Namen adressiert werden. Für die Überprüfung der Namen gibt es keine zentrale Instanz. Jeder Computer im Netzwerk kann beliebig viele Namen reservieren, solange die Namen noch nicht Gebrauch sind. Die NetBIOS-Schnittstelle kann in unterschiedlichen Netzwerkarchitekturen implementiert werden. Eine Implementierung, die relativ eng mit der Netzwerkhardware arbeitet, ist NetBEUI (häufig auch als NetBIOS bezeichnet). Mit NetBIOS implementierte Netzwerkprotokolle sind IPX (NetBIOS über TCP/IP) von Novell und TCP/IP.

  Die per TCP/IP übermittelten NetBIOS-Namen haben nichts mit den in der Datei `/etc/hosts` oder per DNS vergebenen Namen zu tun. NetBIOS ist ein eigener, vollständig unabhängiger Namensraum. Es empfiehlt sich jedoch, für eine einfachere Administration NetBIOS-Namen zu vergeben, die den jeweiligen DNS-Hostnamen entsprechen, oder DNS nativ zu verwenden. Für einen Samba-Server ist dies die Voreinstellung.

Samba-Server
: Samba-Server stellt SMB/CIFS-Dienste sowie NetBIOS over IP-Namensdienste für Clients zur Verfügung. Für Linux gibt es drei Daemons für Samba-Server: smnd für SMB/CIFS-Dienste, nmbd für Naming Services und winbind für Authentifizierung.

Samba-Client
: Samba-Client ist ein System, das Samba-Dienste von einem Samba-Server über das SMB-Protokoll nutzt. Das Samba-Protokoll wird von allen gängigen Betriebssystemen wie Mac OS X, Windows und OS/2 unterstützt. Auf den Computern muss das TCP/IP-Protokoll installiert sein. Für die verschiedenen UNIX-Versionen stellt Samba einen Client zur Verfügung. Für Linux gibt es zudem ein Dateisystem-Kernel-Modul für SMB, das die Integration von SMB-Ressourcen auf Linux-Systemebene ermöglicht. Sie brauchen für Samba-Client keinen Daemon auszuführen.

Freigaben
: SMB-Server stellen den Clients Ressourcen in Form von Freigaben (Shares) zur Verfügung. Freigaben sind Drucker und Verzeichnisse mit ihren Unterverzeichnissen auf dem Server. Eine Freigabe wird unter einem eigenen Namen exportiert und kann von Clients unter diesem Namen angesprochen werden. Der Freigabename kann frei vergeben werden. Er muss nicht dem Namen des exportierten Verzeichnisses entsprechen. Ebenso wird einem Drucker ein Name zugeordnet. Clients können mit diesem Namen auf den Drucker zugreifen.

DC
: Ein Domain Controller (DC) ist ein Server, der Konten in der Domäne verwaltet. Zur Datenreplikation stehen zusätzliche Domain Controller in einer Domäne zur Verfügung.

24.2 Starten und Stoppen von Samba

Sie können den Samba-Server automatisch beim Booten oder manuell starten bzw. stoppen. Start- und Stopprichtlinien sind Teil der Samba-Serverkonfiguration mit YaST, die in Abschnitt 24.3.1, „Konfigurieren eines Samba-Servers mit YaST“ (S. 378) beschrieben wird.

Um Samba-Dienste mit YaST zu stoppen oder zu starten, verwenden Sie *System* > *Systemdienste (Runlevel-Editor)* und wählen Sie winbind, smb und nmb. In der Kommandozeile stoppen Sie für Samba erforderliche Dienste mit `rcsmb stop && rcnmb stop` und starten sie mit `rcnmb start && rcsmb start`; bei Bedarf kümmert sich rcsmb um winbind.

24.3 Konfigurieren eines Samba-Servers

Es gibt zwei Möglichkeiten, Samba-Server in SUSE® Linux Enterprise Server zu konfigurieren: mit YaST oder manuell. Bei der manuellen Konfiguration können Sie mehr Details einstellen, allerdings müssen Sie ohne den Komfort der Bedienoberfläche von YaST zurechtkommen.

24.3.1 Konfigurieren eines Samba-Servers mit YaST

Um einen Samba-Server zu konfigurieren, starten Sie YaST und wählen Sie *Netzwerkdienste* > *Samba-Server*.

Anfängliche Samba-Konfiguration

Beim ersten Start des Moduls wird das Dialogfeld *Samba-Installation* geöffnet, das Sie auffordert, ein paar grundlegende Entscheidungen hinsichtlich der Serveradministration zu treffen, und Sie am Ende der Konfiguration nach dem Passwort für Samba-root fragt. Bei späteren Starts wird das Dialogfeld *Samba-Server-Konfiguration* geöffnet.

Der Dialog *Samba-Installation* umfasst zwei Schritte und optionale detaillierte Einstellungen:

Arbeitsgruppe oder Domäne
: Wählen Sie unter *Arbeitsgruppe oder Domäne* eine Arbeitsgruppe oder Domäne aus oder geben Sie eine neue ein und klicken Sie auf *Weiter*.

Samba-Servertyp
: Geben Sie im nächsten Schritt an, ob Ihr Server als CD (PDC) fungieren soll, und klicken Sie auf *Weiter*.

Start
: Wählen Sie, ob Samba *Beim Systemstart* oder *Manuell* gestartet werden soll, und klicken Sie auf *OK*. Legen Sie dann im abschließenden Popup-Feld das *root-Passwort für Samba* fest.

Sie können alle Einstellungen später im Dialogfeld *Samba-Konfiguration* mit den Karteireitern *Start*, *Freigaben* und *Identität* ändern.

Erweiterte Samba-Konfiguration

Beim ersten Start des Samba-Servermoduls wird das Dialogfeld *Samba-Konfiguration* direkt nach den beiden Anfangsschritten (siehe „Anfängliche Samba-Konfiguration“ (S. 378)) geöffnet. Hier passen Sie Ihre Samba-Server-Konfiguration an.

Klicken Sie nach dem Bearbeiten Ihrer Konfiguration auf *OK*, um Ihre Einstellungen zu speichern.

Starten des Servers

Auf dem Karteireiter *Start* können Sie den Start des Samba-Servers konfigurieren. Um den Dienst bei jedem Systemboot zu starten, wählen Sie *During Boot* (Beim Systemstart). Um den manuellen Start zu aktivieren, wählen Sie *Manually* (Manuell). Weitere Informationen zum Starten eines Samba-Servers erhalten Sie in Abschnitt 24.2, „Starten und Stoppen von Samba“ (S. 377).

Auf diesem Karteireiter können Sie auch Ports in Ihrer Firewall öffnen. Wählen Sie hierfür *Open Port in Firewall* (Firewall-Port öffnen). Wenn mehrere Netzwerkschnittstellen vorhanden sind, wählen Sie die Netzwerkschnittstelle für Samba-Dienste, indem Sie auf *Firewall-Details* klicken, die Schnittstellen auswählen und dann auf *OK* klicken.

Freigaben

Legen Sie auf dem Karteireiter *Freigaben* die zu aktivierenden Samba-Freigaben fest. Es gibt einige vordefinierte Freigaben wie Home-Verzeichnisse und Drucker. Mit *Status wechseln* können Sie zwischen den Statuswerten *Aktiviert* und *Deaktiviert* wechseln. Klicken Sie auf *Hinzufügen*, um neue Freigaben hinzuzufügen, bzw. auf *Löschen*, um die ausgewählte Freigabe zu entfernen.

Mit *Benutzern die Freigabe ihrer Verzeichnisse erlauben* können Mitglieder der Gruppe in *Zulässige Gruppe* ihre eigenen Verzeichnisse für andere Benutzer freigeben. Zum Beispiel `users` für eine lokale Reichweite oder `DOMAIN\Users` für eine domänenweite Freigabe. Der Benutzer muss außerdem sicherstellen, dass die Berechtigungen des Dateisystems den Zugriff zulassen. Mit *Maximale Anzahl an Freigaben* begrenzen Sie die Gesamtzahl der erstellbaren Freigaben. Wenn Sie den Zugriff auf Benutzerfreigaben ohne Authentifizierung zulassen möchten, aktivieren Sie *Gastzugriff erlauben*.

Identität

Auf dem Karteireiter *Identität* legen Sie fest, zu welcher Domäne der Host gehört (*Grundeinstellungen*) und ob ein alternativer Hostname im Netzwerk (*NetBIOS-Hostname*) verwendet werden soll. Microsoft Windows Internet Name Service (WINS) kann auch zur Namensauflösung benutzt werden. Aktivieren Sie in diesem Fall *WINS zur Hostnamenauflösung verwenden* und entscheiden Sie, ob Sie *WINS-Server via DHCP*

abrufen möchten. Globale Einstellungen für Experten oder die Benutzerauthentifizierung, beispielsweise LDAP, können Sie festlegen, wenn Sie auf *Erweiterte Einstellungen* klicken.

Benutzer anderer Domänen

Sie ermöglichen Benutzern anderer Domänen den Zugriff auf Ihre Domäne, indem Sie die entsprechenden Einstellungen in dem Karteireiter *Verbürgte Domänen* vornehmen. Klicken Sie zum Hinzufügen einer neuen Domäne auf *Hinzufügen*. Zum Entfernen der ausgewählten Domäne klicken Sie auf *Löschen*.

Verwenden von LDAP

In dem Karteireiter *LDAP-Einstellungen* können Sie den LDAP-Server für die Authentifizierung festlegen. Um die Verbindung mit Ihrem LDAP-Server zu testen, klicken Sie auf *Verbindung testen*. LDAP-Einstellungen für Experten oder die Verwendung von Standardwerten können Sie festlegen, wenn Sie auf *Erweiterte Einstellungen* klicken.

Weitere Informationen zur LDAP-Konfiguration finden Sie unter Kapitel 5, *LDAP—A Directory Service* (↑*Security Guide*).

24.3.2 Web-Administration mit SWAT

SWAT (Samba Web Administration Tool) ist ein alternativesWerkzeug für die Administrationsaufgaben von Samba. Es stellt eine einfache Webschnittstelle zur Verfügung, mit der Sie den Samba-Server konfigurieren können. Sie können SWAT verwenden, indem Sie in einem Webbrowser `http://localhost:901` aufrufen und sich als `root` anmelden. Wenn Sie über kein spezielles root-Konto für Samba verfügen, verwenden Sie das `root`-Systemkonto.

ANMERKUNG: Aktivieren von SWAT

Nach der Installation von Samba-Server ist SWAT nicht aktiviert. Um SWAT zu aktivieren, öffnen Sie in YaST *Netzwerkdienste* > *Netzwerkdienste (xinetd)*, wählen Sie *swat* aus der Tabelle und klicken Sie auf *Status wechseln (Ein oder Aus)*.

24.3.3 Manuelles Konfigurieren des Servers

Wenn Sie Samba als Server verwenden möchten, installieren Sie `samba`. Die Hauptkonfigurationsdatei von Samba ist `/etc/samba/smb.conf`. Diese Datei kann in zwei logische Bereiche aufgeteilt werden. Der Abschnitt `[global]` enthält die zentralen und globalen Einstellungen. Die Abschnitte `[share]` enthalten die einzelnen Datei- und Druckerfreigaben. Mit dieser Vorgehensweise können Details der Freigaben unterschiedlich oder im Abschnitt `[global]` übergreifend festgelegt werden. Letzteres trägt zur Übersichtlichkeit der Konfigurationsdatei bei.

Der Abschnitt "global"

Die folgenden Parameter im Abschnitt `[global]` sind den Gegebenheiten Ihres Netzwerkes anzupassen, damit Ihr Samba-Server in einer Windows-Umgebung von anderen Computern über SMB erreichbar ist.

workgroup = TUX-NET
: Mit dieser Zeile wird der Samba-Server einer Arbeitsgruppe zugeordnet. Ersetzen Sie `TUX-NET` durch eine entsprechende Arbeitsgruppe Ihrer Netzwerkumgebung. Der Samba-Server erscheint mit seinem DNS-Namen, sofern der Name noch nicht vergeben ist. Wenn der DNS-Name nicht verfügbar ist, kann der Servername mithilfe von `netbiosname=`*`MEINNAME`* festgelegt werden. Weitere Details zu diesem Parameter finden Sie auf der man-Seite `smb.conf`.

os level = 2
: Anhand dieses Parameters entscheidet Ihr Samba-Server, ob er versucht, LMB (Local Master Browser) für seine Arbeitsgruppe zu werden. Wählen Sie bewusst einen niedrigen Wert, damit ein vorhandenes Windows-Netz nicht durch einen falsch konfigurierten Samba-Server gestört wird. Weitere Informationen zu diesem wichtigen Thema finden Sie in den Dateien `BROWSING.txt` und `BROWSING-Config.txt` im Unterverzeichnis `textdocs` der Paketdokumentation.

  Wenn im Netzwerk kein anderer SMB-Server (z. B. ein Windows 2000-Server) vorhanden ist und der Samba-Server eine Liste aller in der lokalen Umgebung vorhandenen Systeme verwalten soll, setzen Sie den Parameter `os level` auf einen höheren Wert (z. B. `65`). Der Samba-Server wird dann als LMB für das lokale Netzwerk ausgewählt.

Beim Ändern dieses Werts sollten Sie besonders vorsichtig sein, da dies den Betrieb einer vorhandenen Windows-Netzwerkumgebung stören könnte. Testen Sie Änderungen zuerst in einem isolierten Netzwerk oder zu unkritischen Zeiten.

wins support und wins server
: Wenn Sie den Samba-Server in ein vorhandenes Windows-Netzwerk integrieren möchten, in dem bereits ein WINS-Server betrieben wird, aktivieren Sie den Parameter `wins server` und setzen Sie seinen Wert auf die IP-Adresse des WINS-Servers.

  Sie müssen einen WINS-Server einrichten, wenn Ihre Windows-Systeme in getrennten Subnetzen betrieben werden und sich gegenseitig erkennen sollen. Um einen Samba-Server als WINS-Server festzulegen, setzen Sie die Option `wins support = Yes`. Stellen Sie sicher, dass diese Einstellung nur auf einem einzigen Samba-Server im Netzwerk aktiviert wird. Die Optionen `wins server` und `wins support` dürfen in der Datei `smb.conf` niemals gleichzeitig aktiviert sein.

Freigaben

In den folgenden Beispielen werden einerseits das CD-ROM-Laufwerk und andererseits die Verzeichnisse der Nutzer (`homes`) für SMB-Clients freigegeben.

[cdrom]
: Um die versehentliche Freigabe eines CD-ROM-Laufwerks zu verhindern, sind alle erforderlichen Zeilen dieser Freigabe durch Kommentarzeichen (hier Semikolons) deaktiviert. Entfernen Sie die Semikolons in der ersten Spalte, um das CD-ROM-Laufwerk für Samba freizugeben.

Beispiel 24.1 *Eine CD-ROM-Freigabe (deaktiviert)*

```
;[cdrom]
;       comment = Linux CD-ROM
;       path = /media/cdrom
;       locking = No
```

`[cdrom]` und `comment`
: Der Eintrag `[cdrom]` ist der Name der Freigabe, die von allen SMB-Clients im Netzwerk gesehen werden kann. Zur Beschreibung dieser Freigabe kann ein zusätzlicher `comment` hinzugefügt werden.

`path = /media/cdrom`
: `path` exportiert das Verzeichnis `/media/cdrom`.

Diese Art der Freigabe ist aufgrund einer bewusst restriktiv gewählten Voreinstellung lediglich für die auf dem System vorhandenen Benutzer verfügbar. Soll die Freigabe für alle Benutzer bereitgestellt werden, fügen Sie der Konfiguration die Zeile `guest ok = yes` hinzu. Durch diese Einstellung erhalten alle Benutzer im Netzwerk Leseberechtigungen. Es wird empfohlen, diesen Parameter sehr vorsichtig zu verwenden. Dies gilt umso mehr für die Verwendung dieses Parameters im Abschnitt `[global]`.

`[homes]`
: Eine besondere Stellung nimmt die Freigabe `[homes]` ein. Hat der Benutzer auf dem Linux-Dateiserver ein gültiges Konto und ein eigenes Home-Verzeichnis, so kann er eine Verbindung zu diesem herstellen.

Beispiel 24.2 *homes-Freigabe*

```
[homes]
 comment = Home Directories
 valid users = %S
 browseable = No
 read only = No
 create mask = 0640
 directory mask = 0750
```

[homes]
: Insoweit keine ausdrückliche Freigabe mit dem Freigabenamen des Benutzers existiert, der die Verbindung zum SMB-Server herstellt, wird aufgrund der `[homes]`-Freigabe dynamisch eine Freigabe generiert. Dabei ist der Freigabename identisch mit dem Benutzernamen.

`valid users = %S`
: `%S` wird nach erfolgreichem Verbindungsaufbau durch den konkreten Freigabenamen ersetzt. Bei einer `[homes]`-Freigabe ist dies immer der Benutzername. Aus diesem Grund werden die Zugriffsberechtigungen auf die Freigabe eines Benutzers immer exklusiv auf den Eigentümer des Benutzerverzeichnisses beschränkt.

`browseable = No`
: Durch diese Einstellung wird die Freigabe in der Netzwerkumgebung unsichtbar gemacht.

`read only = No`
: Samba untersagt Schreibzugriff auf exportierte Freigaben standardmäßig mit dem Parameter `read only = Yes`. Soll also ein Verzeichnis als schreibbar freigegeben werden, muss der Wert `read only = No` festgesetzt werden, was dem Wert `writeable = Yes` entspricht.

`create mask = 0640`
: Nicht auf MS Windows NT basierende Systeme kennen das Konzept der Unix-Zugriffsberechtigungen nicht, sodass sie beim Erstellen einer Datei keine Berechtigungen zuweisen können. Der Parameter `create mask` legt fest, welche Zugriffsberechtigungen neu erstellten Dateien zugewiesen werden. Dies gilt jedoch nur für Freigaben mit Schreibberechtigung. Konkret wird hier dem Eigentümer das Lesen und Schreiben und den Mitgliedern der primären Gruppe des Eigentümers das Lesen erlaubt. `valid users = %S` verhindert den Lesezugriff auch dann, wenn die Gruppe über Leseberechtigungen verfügt. Um der Gruppe Lese- oder Schreibzugriff zu gewähren, deaktivieren Sie die Zeile `valid users = %S`.

Sicherheitsstufen (Security Levels)

Jeder Zugriff auf eine Freigabe kann für mehr Sicherheit durch ein Passwort geschützt werden. SMB kennt vier verschiedene Möglichkeiten der Berechtigungsprüfung:

Share Level Security (security = share)
: Einer Freigabe wird ein Passwort fest zugeordnet. Jeder Benutzer, der dieses Passwort kennt, hat Zugriff auf die Freigabe.

User Level Security (security = user)
: Diese Variante führt das Konzept des Benutzers in SMB ein. Jeder Benutzer muss sich bei einem Server mit einem Passwort anmelden. Nach der Authentifizierung kann der Server dann abhängig vom Benutzernamen Zugriff auf die einzelnen exportierten Freigaben gewähren.

Server Level Security (security = server)
: Seinen Clients gibt Samba vor, im User Level Mode zu arbeiten. Allerdings übergibt es alle Passwortanfragen an einen anderen User Level Mode Server, der die Authentifizierung übernimmt. Diese Einstellung erwartet einen weiteren Parameter (`password server`).

Sicherheit der Stufe ADS (Sicherheit = ADS)
: In diesem Modus fungiert Samba als Domänenmitglied in einer Active Directory-Umgebung. Für den Betrieb in diesem Modus muss auf dem Computer, auf dem Samba ausgeführt wird, Kerberos installiert und konfiguriert sein. Der Computer, auf dem Samba verwendet wird, muss in den ADS-Bereich integriert sein. Dies kann mithilfe des YaST-Moduls *Windows-Domänenmitgliedschaft* erreicht werden.

Domain Level Security (security = domain)
: Dieser Modus funktioniert nur korrekt, wenn der Computer in eine Windows NT-Domäne integriert wurde. Samba versucht, den Benutzernamen und das Passwort zu validieren, indem es diese an einen Window NT-Primär-Controller oder Backup Domain Controller weiterleitet. Ein Windows NT-Server wäre ausreichend. Er erwartet, dass der Parameter für das verschlüsselte Passwort auf `ja` festgelegt wurde.

Die Sicherheit auf Freigabe-, Benutzer-, Server- und Domänenebene (Share, User, Server und Domain Level Security) gilt für den gesamten Server. Es ist nicht möglich, einzelne Freigaben einer Serverkonfiguration mit Share Level Security und andere mit User Level Security zu exportieren. Sie können jedoch auf einem System für jede konfigurierte IP-Adresse einen eigenen Samba-Server ausführen.

Weitere Informationen zu diesem Thema finden Sie in der Samba-HOWTO-Collection. Wenn sich mehrere Server auf einem System befinden, beachten Sie die Optionen `interfaces` und `bind interfaces only`.

24.4 Konfigurieren der Clients

Clients können auf den Samba-Server nur über TCP/IP zugreifen. NetBEUI oder NetBIOS über IPX können mit Samba nicht verwendet werden.

24.4.1 Konfigurieren eines Samba-Clients mit YaST

Konfigurieren Sie einen Samba-Client, um auf Ressourcen (Dateien oder Drucker) auf dem Samba-Server zuzugreifen. Geben Sie im Dialogfeld *Netzwerkdienste* > *Windows-Domänenmitgliedschaft* die Domäne oder Arbeitsgruppe an. Wenn Sie *Zusätzlich SMB-Informationen für Linux-Authentifikation verwenden* aktivieren, erfolgt die Benutzerau-

thentifizierung über den Samba-Server. Wenn Sie alle Einstellungen vorgenommen haben, klicken Sie auf *Verlassen*, um die Konfiguration abzuschließen.

24.5 Samba als Anmeldeserver

In Netzwerken, in denen sich überwiegend Windows-Clients befinden, ist es oft wünschenswert, dass sich Benutzer nur mit einem gültigen Konto und zugehörigem Passwort anmelden dürfen. In einem Windows-basierten Netzwerk wird diese Aufgabe von einem Primary Domain Controller (PDC) übernommen. Sie können einen Windows NT-Server verwenden, der als PDC konfiguriert wurde, aber diese Aufgabe kann auch mithilfe eines Samba-Servers erfolgen. Es müssen Einträge im Abschnitt `[global]` von `smb.conf` vorgenommen werden. Diese werden in Beispiel 24.3, „Abschnitt "global" in smb.conf“ (S. 386) beschrieben.

Beispiel 24.3 *Abschnitt "global" in smb.conf*

```
[global]
    workgroup = TUX-NET
    domain logons = Yes
    domain master = Yes
```

Wenn verschlüsselte Passwörter zur Verifizierung verwendet werden, muss der Samba-Server in der Lage sein, diese zu verwalten. Dies wird durch den Eintrag `encrypt passwords = yes` im Abschnitt `[global]` aktiviert (ab Samba Version 3 ist dies Standard). Außerdem müssen die Benutzerkonten bzw. die Passwörter in eine Windows-konforme Verschlüsselungsform gebracht werden. Verwenden Sie hierfür den Befehl `smbpasswd -a name`. Da nach dem Windows-Domänenkonzept auch die Computer selbst ein Domänenkonto benötigen, wird dieses mit den folgenden Kommandos angelegt:

Beispiel 24.4 *Einrichten eines Computerkontos*

```
useradd hostname\$
smbpasswd -a -m hostname
```

Mit dem Befehl `useradd` wird ein Dollarzeichen hinzugefügt. Der Befehl `smbpasswd` fügt dieses bei der Verwendung des Parameters `-m` automatisch hinzu. In der kommentierten Beispielkonfiguration (`/usr/share/doc/packages/Samba/examples/smb.conf.SuSE`) sind Einstellungen enthalten, die diese Arbeiten automatisieren.

Beispiel 24.5 *Automatisiertes Einrichten eines Computerkontos*

```
add machine script = /usr/sbin/useradd -g nogroup -c "NT Machine Account" \
-s /bin/false %m\$
```

Damit dieses Skript von Samba richtig ausgeführt werden kann, benötigen Sie noch einen Samba-Benutzer mit Administratorrechten. Fügen Sie hierzu der Gruppe `ntadmin` einen entsprechenden Benutzer hinzu. Anschließend können Sie allen Mitgliedern der Linux-Gruppe den Status `Domain Admin` zuweisen, indem Sie folgenden Befehl eingeben:

```
net groupmap add ntgroup="Domain Admins" unixgroup=ntadmin
```

Weitere Informationen zu diesem Thema finden Sie in Kapitel 12 der Samba-HOWTO-Collection (`/usr/share/doc/packages/samba/Samba-HOWTO-Collection.pdf`).

24.6 Samba-Server im Netzwerk mit Active Directory

Wenn Sie Linux- und Windows-Server gemeinsam ausführen, können Sie zwei unabhängige Authentifizierungssysteme und -netzwerke aufbauen oder die Server mit einem Netzwerk verbinden, das über ein zentrales Authentifizierungssystem verfügt. Da Samba mit einer Active Directory-Domäne zusammenarbeitet, können Sie Ihr SUSE Linux Enterprise Server mit Active Directory (AD) anbinden.

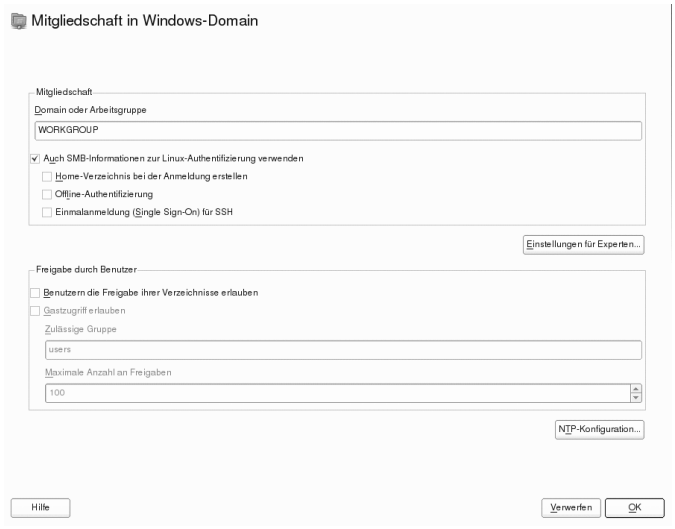
Binden Sie eine vorhandene AD-Domäne während der Installation an oder indem Sie später die SMB-Benutzerauthentifizierung mit YaST im installierten System aktivieren. Genauere Informationen zur Domänenanbindung während der Installation finden Sie unter „Benutzerbeglaubigungsmethode“ (Kapitel 6, *Installation mit YaST*, ↑*Bereitstellungshandbuch*).

Zum Anbinden einer AD-Domäne in einem laufenden System gehen Sie wie folgt vor:

1. Melden Sie sich als `root` an und starten Sie YaST.
2. Starten Sie *Netzwerkdienste* > *Windows-Domänenmitgliedschaft*.

3 Geben Sie die zu verbindende Domäne unter *Domäne oder Arbeitsgruppe* im Dialogfeld *Windows-Domänenmitgliedschaft* an.

Abbildung 24.1 *Festlegen der Windows-Domänenmitgliedschaft*



4 Aktivieren Sie *Zusätzlich SMB-Informationen für Linux-Authentifikation verwenden*, um die SMB-Quelle für die Linux-Authentifizierung unter SUSE Linux Enterprise Server zu nutzen.

5 Klicken Sie auf *OK* und bestätigen Sie nach Aufforderung die Domänenverbindung.

6 Geben Sie das Passwort für den Windows-Administrator auf dem AD-Server an und klicken Sie auf *OK*.

Ihr Server ist jetzt so eingerichtet, dass alle Authentifizierungsdaten vom Active Directory-Domänencontroller abgerufen werden.

24.7 Weiterführende Informationen

Ausführliche Informationen zu Samba finden Sie in der digitalen Dokumentation. Wenn Samba installiert ist, können Sie in der Kommandozeile `apropos samba` eingeben, um einige man-Seiten aufzurufen. Alternativ dazu finden Sie im Verzeichnis `/usr/share/doc/packages/samba` weitere Online-Dokumentationen und Beispiele. Eine kommentierte Beispielkonfiguration (`smb.conf.SuSE`) finden Sie im Unterverzeichnis `examples`.

Das Samba-Team liefert in der Samba-HOWTO-Collection einen Abschnitt zur Fehlerbehebung. In Teil V ist außerdem eine ausführliche Anleitung zum Überprüfen der Konfiguration enthalten. Nach der Installation des Pakets `samba-doc` finden Sie die HOWTO-Informationen im Verzeichnis `/usr/share/doc/packages/samba/Samba-HOWTO-Collection.pdf`.

Lesen Sie auch die Samba-Seite im openSUSE-wiki unter `http://en.openSUSE.org/Samba`.

Verteilte Nutzung von Dateisystemen mit NFS

25

Das Verteilen und Freigeben von Dateisystemen über ein Netzwerk ist eine Standardaufgabe in Unternehmensumgebungen. `NFS` ist ein bewährtes System, das auch mit dem Yellow Pages-Protokoll `NIS` zusammenarbeitet. Wenn Sie ein sichereres Protokoll wünschen, das mit `LDAP` zusammenarbeitet und auch kerberisiert werden kann, aktivieren Sie `NFSv4`.

NFS dient neben NIS dazu, ein Netzwerk für den Benutzer transparent zu machen. Mit NFS ist es möglich, arbiträre Dateisysteme über das Netzwerk zu verteilen. Bei entsprechendem Setup befinden sich Benutzer in derselben Umgebung, unabhängig vom gegenwärtig verwendeten Terminal.

Wie NIS ist NFS ein Client-Server-System. Ein Computer kann jedoch beides gleichzeitig sein – er kann Dateisysteme im Netzwerk zur Verfügung stellen (exportieren) und Dateisysteme anderer Hosts einhängen (importieren).

WICHTIG: DNS-Bedarf

Im Prinzip können alle Exporte allein mit IP-Adressen vorgenommen werden. Es ist ratsam, über ein funktionierendes DNS-System zu verfügen, um Zeitüberschreitungen zu vermeiden. Dies ist zumindest für die Protokollierung erforderlich, weil der mountd-Daemon Reverse-Lookups ausführt.

25.1 Installieren der erforderlichen Software

Wenn Sie Ihren Host als NFS-Client konfigurieren möchten, müssen Sie keine zusätzliche Software installieren. Alle erforderlichen Pakete für die Konfiguration eines NFS-Client werden standardmäßig installiert.

NFS-Server-Software ist kein Bestandteil der Standardinstallation. Zur Installation der NFS-Server-Software starten Sie YaST und wählen Sie *Software* > *Software installieren oder löschen* aus. Wählen Sie nun *Filter* > *Schemata* und anschließend *Verschiedene Server* aus. Oder verwenden Sie die Option *Suchen* und suchen Sie nach `NFS-Server`. Bestätigen Sie die Installation der Pakete, um den Installationsvorgang abzuschließen.

25.2 Importieren von Dateisystemen mit YaST

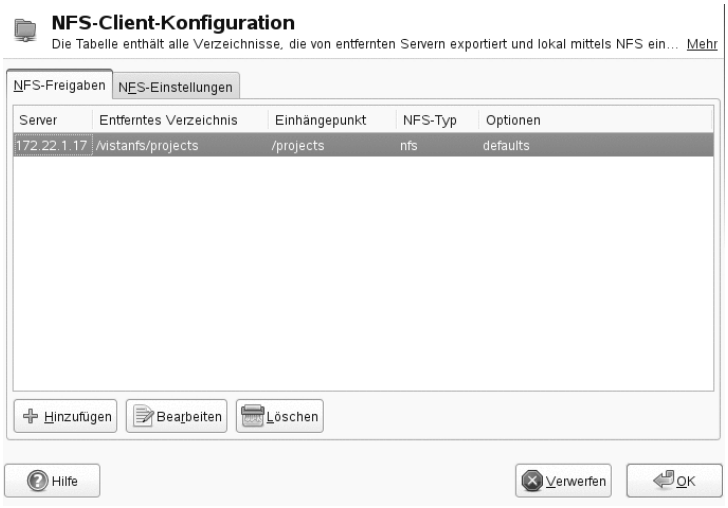
Autorisierte Benutzer können NFS-Verzeichnisse von NFS-Servern in ihre eigenen Dateibäume einhängen. Dies geschieht mit dem YaST-Modul *NFS-Client*. Klicken Sie auf *Hinzufügen* und geben Sie nur den Hostnamen des NFS-Servers, das zu importierende Verzeichnis und den Einhängepunkt an, an dem das Verzeichnis lokal eingehängt werden soll. Die Änderungen werden wirksam, nachdem im ersten Dialogfeld auf *Beenden* geklickt wird.

Klicken Sie auf dem Karteireiter *NFS-Einstellungen* auf *Firewall-Port öffnen*, um die Firewall zu öffnen und entfernten Computern den Zugriff auf den Dienst zu gewähren. Der Status der Firewall wird neben dem Kontrollkästchen angezeigt. Wenn Sie NFSv4 verwenden, vergewissern Sie sich, dass das Kontrollkästchen für *NFSv4 aktivieren* aktiviert ist, und dass der *NFSv4-Domänenname* denselben Wert enthält, den der NFSv4-Server verwendet. Die Standarddomäne ist `localdomain`.

Klicken Sie zum Speichern der Änderungen auf *Beenden*. Weitere Informationen hierzu finden Sie unter Abbildung 25.1, „Konfiguration des NFS-Clients mit YaST“ (S. 393).

Die Konfiguration wird in `/etc/fstab` geschrieben und die angegebenen Dateisysteme werden eingehängt. Wenn Sie den YaST-Konfigurationsclient zu einem späteren Zeitpunkt starten, wird auch die vorhandene Konfiguration aus dieser Datei gelesen.

Abbildung 25.1 *Konfiguration des NFS-Clients mit YaST*



25.3 Manuelles Importieren von Dateisystemen

Dateien können auch manuell von einem NFS-Server importiert werden. Die Voraussetzung dafür ist, dass ein RPC-Portmapper ausgeführt wird, der durch die Eingabe von `rcrpcbind start` als `root` gestartet werden kann. Sobald diese Voraussetzung erfüllt ist, können entfernt exportierte Dateisysteme genau wie lokale Festplatten mithilfe des Befehls `Einhängen` auf folgende Weise im Dateisystem eingehängt werden:

```
mount host:remote-path local-path
```

Wenn beispielsweise Benutzerverzeichnisse vom Computer nfs.example.com importiert werden sollen, lautet das Kommando:

```
mount nfs.example.com:/home /home
```

25.3.1 Verwenden des Diensts zum automatischen Einhängen

Genau wie die regulären Einhängungen für lokale Geräte kann auch der autofs-Daemon zum automatischen Einhängen von entfernten Dateisystemen verwendet werden. Fügen Sie dazu den folgenden Eintrag in der Datei `/etc/auto.master` hinzu:

```
/nfsmounts /etc/auto.nfs
```

Nun fungiert das Verzeichnis `/nfsmounts` als Root-Verzeichnis für alle NFS-Einhängungen auf dem Client, wenn die Datei `auto.nfs` entsprechend beendet wurde. Der Name `auto.nfs` wurde nur der Einfachheit halber ausgewählt – Sie können einen beliebigen Namen auswählen. Fügen Sie der ausgewählten Datei (erstellen Sie diese, wenn sie nicht vorhanden ist) Einträge für alle NFS-Einhängungen wie im folgenden Beispiel dargestellt hinzu:

```
localdata –fstype=nfs server1:/data
nfs4mount –fstype=nfs4 server2:/
```

Aktivieren Sie die Einstellungen mit `rcautofs start`. In diesem Beispiel wird `/nfsmounts/localdata`, das Verzeichnis `/data` von server1, mit NFS eingehängt und `/nfsmounts/nfs4mount` von server2 wird mit NFSv4 eingehängt.

Wenn die Datei `/etc/auto.master` während dem Ausführen des Diensts autofs bearbeitet wird, muss die automatische Einhängung erneut gestarted werden, damit die Änderungen wirksam werden. Verwenden Sie dazu den Befehl `rcautofs restart`.

25.3.2 Manuelles Bearbeiten von /ect/fstab

Ein typischer NFSv3-Einhängeeintrag in `/etc/fstab` sieht folgendermaßen aus:

```
nfs.example.com:/data /local/path nfs rw,noauto 0 0
```

NFSv4-Einhängungen können der Datei `/etc/fstab` auch manuell hinzugefügt werden. Verwenden Sie für diese Einhängungen in der dritten Spalte `nfs4` statt `nfs` und stellen Sie sicher, dass das entfernte Dateisystem in der ersten Spalte nach *`nfs.example.com`* als `/` angegeben ist. Eine typische Zeile für eine NFSv4-Einhängung in `/etc/fstab` sieht zum Beipsiel wie folgt aus:

```
nfs.example.com:/ /local/pathv4 nfs4 rw,noauto 0 0
```

Mit der Option `noauto` wird verhindert, dass das Dateisystem beim Starten automatisch eingehängt wird. Wenn Sie das jeweilige Dateisystem manuell einhängen möchten, können Sie das Einhängekommando auch kürzen. Es muss in diesem Fall wie das folgende Kommando nur den Einhängepunkt angeben:

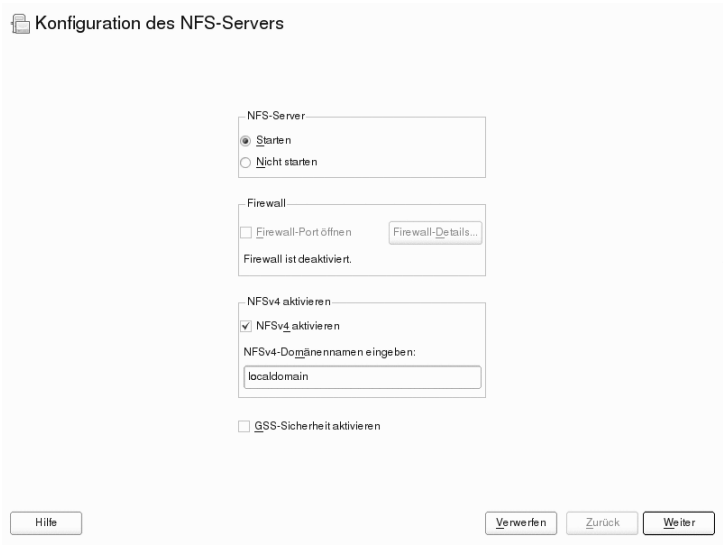
```
mount /local/path
```

Beachten Sie, dass das Einhängen dieser Dateisysteme beim Start durch die Initialisierungsskripte des Systems geregelt wird, wenn die Option `noauto` nicht angegeben ist.

25.4 Exportieren von Dateisystemen mit YaST

Mit YaST können Sie einen Computer im Netzwerk als NFS-Server bereitstellen. Dies ist ein Server, der Verzeichnisse und Dateien an alle Hosts exportiert, die ihm Zugriff gewähren. Auf diese Weise können Anwendungen für alle Mitglieder einer Gruppe zur Verfügung gestellt werden, ohne dass sie lokal auf deren Hosts installiert werden müssen. Starten Sie zum Installieren eines solchen Servers YaST und wählen Sie *Netzwerkdienste* > *NFS-Server* aus. Ein Dialogfeld wie in Abbildung 25.2, „Konfiguration des NFS-Servers“ (S. 396) wird geöffnet.

Abbildung 25.2 *Konfiguration des NFS-Servers*



Aktivieren Sie dann *NFS-Server starten* und geben Sie den *NFSv4-Domänennamen* ein.

Klicken Sie auf *GSS-Sicherheit aktivieren*, wenn Sie einen sicheren Zugriff auf den Server benötigen. Als Voraussetzung hierfür muss Kerberos in der Domäne installiert sein und sowohl der Server als auch der Client müssen kerberisiert sein. Klicken Sie auf *Weiter*.

Geben Sie im oberen Textfeld die zu exportierenden Verzeichnisse an. Legen Sie darunter Hosts fest, die darauf Zugriff erhalten sollen. Dieses Dialogfeld ist in Abbildung 25.3, „Konfigurieren eines NFS-Servers mit YaST“ (S. 397) abgebildet. In der Abbildung wird das Szenario dargestellt, bei dem NFSv4 im vorherigen Dialogfeld aktiviert wurde. `Einhängeziele binden` wird in der rechten Leiste angezeigt. Weitere Details finden Sie in der Hilfe auf der rechten Leiste. In der unteren Hälfte des Dialogfelds befinden sich vier Optionen, die für jeden Host festgelegt werden können: `single host (Einzelhost)`, `netgroups (Netzgruppen)`, `wildcards (Platzhalterzeichen)` und `IP-Netzwerke`. Eine ausführlichere Erläuterung zu diesen Optionen finden Sie auf der man-Seite über `Exporte`. Klicken Sie zum Beenden der Konfiguration auf *Beenden*.

Abbildung 25.3 *Konfigurieren eines NFS-Servers mit YaST*

WICHTIG: Automatische Firewall-Konfiguration

Wenn auf Ihrem System eine Firewall aktiviert ist (SuSEfirewall2), wird deren Konfiguration von YaST für den NFS-Server angepasst, indem der `nfs`-Dienst aktiviert wird, wenn *Firewall-Ports öffnen* ausgewählt ist.

25.4.1 Exportieren für NFSv4-Clients

Aktivieren Sie *NFSv4 aktivieren*, um NFSv4-Clients zu unterstützen. Clients mit NFSv3 können immer noch auf die exportierten Verzeichnisse des Servers zugreifen, wenn diese entsprechend exportiert wurden. Dies wird in Abschnitt 25.4.3, „Gleichzeitig vorhandene v3-Exporte und v4-Exporte“ (S. 400) detailliert beschrieben.

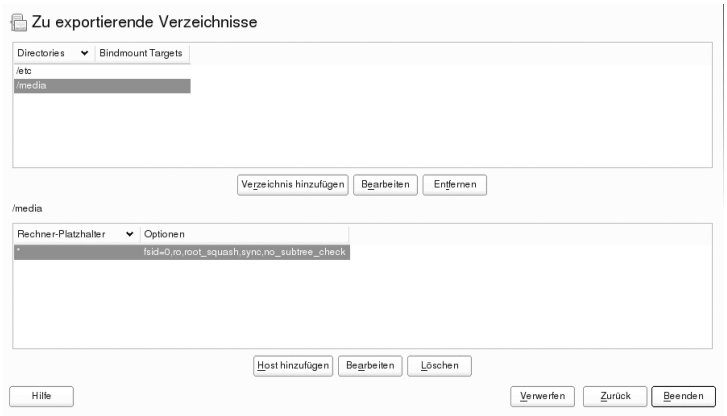
Geben Sie nach dem Aktivieren von NFSv4 einen geeigneten Domänennamen an. Stellen Sie sicher, dass der eingegebene Name dem Namen in der Datei `/etc/idmapd.conf` eines beliebigen NFSv4-Client enspricht, der auf diesen speziellen Server zugreift. Dieser Parameter wird für den idmapd-Dienst verwendet, der für die NFSv4-Unterstützung (auf dem Server und dem Client) erforderlich ist. Behalten Sie den Wert `localdomain` (der Standardwert) bei, wenn Sie keine speziellen Anforderungen

haben. Weitere Informationen finden Sie in Abschnitt 25.7, „Weiterführende Informationen“ (S. 405).

Klicken Sie auf *Weiter*. Das darauf folgende Dialogfeld ist in zwei Abschnitte unterteilt. Die obere Hälfte besteht aus zwei Spalten mit den Namen *Verzeichnisse* und *Einhängeziele binden*. Bei *Verzeichnisse* handelt es sich um eine direkt bearbeitbare Spalte, in der die zu exportierenden Verzeichnisse aufgelistet werden.

Bei einer festen Gruppe von Clients gibt es zwei Arten von Clients, die exportiert werden können – Verzeichnisse, die als Pseudo-Root-Dateisysteme fungieren, und solche, die an ein Unterverzeichnis eines Pseudo-Dateisystems gebunden sind. Dieses Pseudo-Dateisystem stellt den Basispunkt dar, unter dem alle Dateisysteme angeordnet werden, die für dieselbe Gruppe von Clients exportiert wurden. Bei einem Client oder einer Gruppe von Clients kann nur ein Verzeichnis auf dem Server als Pseudo-Root-Verzeichnis für den Export konfiguriert werden. Exportieren Sie für diesen Client mehrere Verzeichnisse, indem Sie sie an vorhandene Unterverzeichnisse im Pseudo-Root-Verzeichnis binden.

Abbildung 25.4 *Exportieren von Verzeichnissen mit NFSv4*



Geben Sie in der unteren Hälfte des Dialogfelds die Export- und Client-Optionen (Platzhalterzeichen) für ein bestimmtes Verzeichnis ein. Nach dem Hinzufügen eines Verzeichnisses in der oberen Hälfte wird automatisch ein weiteres Dialogfeld zum Eingeben von Client- und Optionsinformationen geöffnet. Klicken Sie danach zum Hinzufügen eines neuen Client (einer Gruppe von Clients) auf *Host hinzufügen*.

Geben Sie im kleinen Dialogfeld, das geöffnet wird, das Platzhalterzeichen für den Host ein. Es gibt vier mögliche Typen von Platzhalterzeichen für den Host, die für jeden Host festgelegt werden können: ein einzelner Host (Name oder IP-Adresse), Netzgruppen, Platzhalterzeichen (wie `*`, womit angegeben wird, dass alle Computer auf den Server zugreifen können) und IP-Netzwerke. Schließen Sie dann unter *Optionen* die Zeichenfolge `fsid=0` in die kommagetrennte Liste der Optionen ein, um das Verzeichnis als Pseudo-Root-Verzeichnis zu konfigurieren. Wenn dieses Verzeichnis an ein anderes Verzeichnis unter einem bereits konfigurierten Pseudo-Root-Verzeichnis gebunden werden soll, stellen Sie sicher, dass ein Zielpfad zum Binden mit der Struktur `bind=/target/path` in der Optionsliste angegeben ist.

Nehmen Sie beispielsweise an, dass das Verzeichnis `/exports` als Pseudo-Root-Verzeichnis für alle Clients ausgewählt wurde, die auf den Server zugreifen können. Fügen Sie dies in der oberen Hälfte hinzu und stellen Sie sicher, dass die für dieses Verzeichnis eingebenen Optionen `fsid=0` einschließen. Wenn Sie über ein anderes Verzeichnis, `/data`, verfügen, das auch mit NFSv4 exportiert werden muss, fügen Sie dieses Verzeichnis der oberen Hälfte hinzu. Stellen Sie beim Eingeben von Optionen für dieses Verzeichnis sicher, dass `bind=/exports/data` in der Liste enthalten ist und dass es sich bei `/exports/data` um ein bereits bestehendes Unterverzeichnis von `/exports` handelt. Alle Änderungen an der Option `bind=/target/path` werden unter *Einhängeziele binden* angezeigt, unabhängig davon, ob ein Wert hinzugefügt, gelöscht oder geändert wurde. Bei dieser Spalte handelt es sich nicht um eine direkt bearbeitbare Spalte. In ihr werden stattdessen Verzeichnisse und deren Ursprung zusammengefasst. Nachdem die Informationen vollständig sind, klicken Sie auf *Beenden*, um die Konfiguration abzuschließen, oder auf *Start*, um den Dienst neu zu starten.

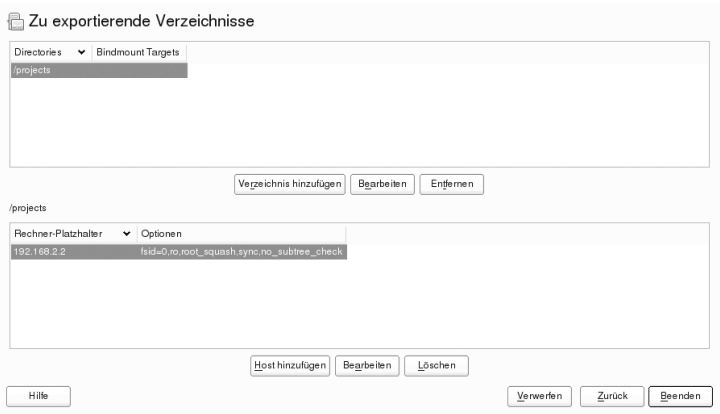
25.4.2 NFSv3- und NFSv2-Exporte

Stellen Sie vor dem Klicken auf *Weiter* sicher, dass *NFSv4 aktivieren* im ersten Dialogfeld nicht aktiviert ist.

Das nächste Dialogfeld besteht aus zwei Bereichen. Geben Sie im oberen Textfeld die zu exportierenden Verzeichnisse an. Legen Sie darunter Hosts fest, die darauf Zugriff erhalten sollen. Es können vier Arten von Host-Platzhalterzeichen für jeden Host festgelegt werden: ein einzelner Host (Name oder IP-Adresse), Netzwerkgruppen, Platzhalterzeichen (z. B. `*`, womit angegeben wird, dass alle Rechner auf den Server zugreifen können) und IP-Netzwerke.

Dieses Dialogfeld ist in Abbildung 25.5, „Exportieren von Verzeichnissen mit NFSv2 und v3“ (S. 400) abgebildet. Eine ausführlichere Erläuterung dieser Optionen finden Sie unter `man exports`. Klicken Sie zum Abschließen der Konfiguration auf *Beenden*.

Abbildung 25.5 *Exportieren von Verzeichnissen mit NFSv2 und v3*



25.4.3 Gleichzeitig vorhandene v3-Exporte und v4-Exporte

NFSv3-Exporte und NFSv4-Exporte können gleichzeitig auf einem Server vorhanden sein. Nach dem Aktivieren der Unterstützung für NFSv4 im ersten Konfigurationsdialogfeld werden diese Exporte, für die `fsid=0` und `bind=/target/path` nicht in der Optionsliste enthalten sind, als v3-Exporte angesehen. Sehen Sie sich das Beispiel in Abbildung 25.3, „Konfigurieren eines NFS-Servers mit YaST“ (S. 397) an. Wenn Sie ein weiteres Verzeichnis (z. B. `/data2`) mit *Hinzufügen: Verzeichnis* hinzufügen und anschließend weder `fsid=0` noch `bind=/target/path` in der entsprechenden Optionsliste aufgeführt wird, fungiert dieser Export als v3-Export.

WICHTIG

Automatische Firewall-Konfiguration

Wenn SuSEfirewall2 auf Ihrem System aktiviert ist, wird deren Konfiguration von YaST für den NFS-Server angepasst, indem der `nfs`-Dienst aktiviert wird, wenn *Firewall-Ports öffnen* ausgewählt ist.

25.5 Manuelles Exportieren von Dateisystemen

Die Konfigurationsdateien für den NFS-Exportdienst lauten `/etc/exports` und `/etc/sysconfig/nfs`. Zusätzlich zu diesen Dateien ist `/etc/idmapd.conf` für die NFSv4-Serverkonfiguration erforderlich. Führen Sie zum Starten bzw. Neustarten der Dienste das Kommando `rcnfsserver restart` aus. Dies startet auch `rpc.idmapd`, wenn NFSv4 in `/etc/sysconfig/nfs` konfiguriert ist. Der NFS-Server ist von einem laufenden RPC-Portmapper abhängig. Starten Sie aus diesem Grund mit `rcrpcbind restart` auch den Portmapper-Dienst bzw. starten Sie ihn neu.

25.5.1 Exportieren von Dateisystemen mit NFSv4

NFSv4 ist die neueste Version des NFS-Protokolls, die auf SUSE Linux Enterprise Server verfügbar ist. Das Konfigurieren der Verzeichnisse für den Export mit NFSv4 unterscheidet sich geringfügig von den früheren NFS-Versionen.

Die /etc/exports-Datei

Diese Datei enthält eine Liste mit Einträgen. Mit jedem Eintrag wird ein Verzeichnis angegeben, das freigegeben wird. Zudem wird angegeben, wie das Verzeichnis freigegeben wird. Ein typischer Eintrag in `/etc/exports` besteht aus:

```
/shared/directory host(option_list)
```

Beispiel:

```
/export 192.168.1.2(rw,fsid=0,sync,crossmnt)
/export/data 192.168.1.2(rw,bind=/data,sync)
```

Hier wird die IP-Adresse `192.168.1.2` verwendet, um den erlaubten Client zu identifizieren. Sie können auch den Namen des Hosts, ein Platzhalterzeichen, mit dem mehrere Hosts angegeben werden (`*.abc.com`, `*` usw.) oder Netzwerkgruppen (`@my-hosts`) verwenden).

Das Verzeichnis, das `fsid=0` angibt, ist speziell, da es die Root des exportierten Dateisystems darstellt. Gelegentlich wird es auch als Pseudo-Root-Dateisystem bezeichnet. Dieses Verzeichnis muss für den fehlerfreien Betrieb mit NFSv4 auch über `crossmnt` verfügen. Alle anderen Verzeichnisse, die über NFSv4 exportiert wurden, müssen unterhalb dieser Position eingehängt werden. Wenn Sie ein Verzeichnis exportieren möchten, das sich normalerweise nicht unter diesem exportierten Root befindet, muss es in den exportierten Baum eingebunden werden. Das ist über die Syntax `bind=` möglich.

Im obigen Beispiel befindet sich `/data` nicht unter dem Verzeichnis `/export`, jedoch möchten wir es trotzdem exportieren. Daher exportieren wir `/export/data` und geben an, dass das Verzeichnis `/data` an diesen Namen gebunden werden soll. Das Verzeichnis `/export/data` muss existieren und sollte normalerweise leer sein.

Beim Einhängen der Clients von diesem Server sollte damit nur `servername:/` anstelle von `servername:/export` eingehängt werden. Es ist nicht erforderlich, auch `servername:/data` einzuhängen. Dieses Verzeichnis erscheint automatisch unter dem Einhängepunkt von `servername:/`.

/etc/sysconfig/nfs

Diese Datei enthält einige Parameter, mit denen das Verhalten des NFSv4-Server-Daemons bestimmt wird. Es ist wichtig, dass der Parameter NFSv4_SUPPORT auf "yes" festgelegt ist. Mit diesem Parameter wird bestimmt, ob der NFS-Server NFSv4-Exporte und -Clients unterstützt.

/etc/idmapd.conf

Jeder Benutzer eines Linux-Rechners verfügt über einen Namen und eine ID. idmapd führt die Name-zu-ID-Zuordnung für NFSv4-Anforderungen an den Server aus und sendet Antworten an den Client. Dies muss auf dem Server und dem Client für NFSv4 ausgeführt werden, da NFSv4 nur Namen für die eigene Kommunikation verwendet.

Stellen Sie sicher, dass Benutzernamen und IDs (uid) Benutzern auf eine einheitliche Weise auf allen Rechnern zugewiesen werden, auf denen möglicherweise Dateisysteme mit NFS freigegeben werden. Dies kann mit NIS, LDAP oder einem beliebigen einheitlichen Domänenauthentifizierungsmechanismus in Ihrer Domäne erreicht werden.

Für eine ordnungsgemäße Funktionsweise muss der Parameter `Domain` für den Client und den Server in dieser Datei identisch festgelegt sein. Wenn Sie sich nicht sicher sind, belassen Sie die Domäne in den Server- und den Clientdateien als `localdomain`. Eine Beispielkonfigurationsdatei sieht folgendermaßen aus:

```
[General]

Verbosity = 0
Pipefs-Directory = /var/lib/nfs/rpc_pipefs
Domain = localdomain

[Mapping]

Nobody-User = nobody
Nobody-Group = nobody
```

Ändern Sie diese Parameter nur, wenn Sie ganz sicher wissen, welche Auswirkungen diese Aktion hat. Weitere Informationen finden Sie auf der man-Seite zu `idmapd` und `idmapd.conf`; `man idmapd`, `man idmapd.conf`.

Starten und Beenden von Apache

Starten Sie den NFS-Serverdienst nach dem Ändern von `/etc/exports` oder `/etc/sysconfig/nfs` mit `rcnfsserver restart` bzw. starten Sie den Dienst neu. Wenn Sie `/etc/idmapd.conf` geändert haben, laden Sie die Konfigurationsdatei erneut mit dem Kommando `killall -HUP rpc.idmapd`.

Wenn dieser Dienst beim Booten gestartet werden soll, führen Sie das Kommando `chkconfig nfsserver on` aus.

25.5.2 Exportieren von Dateisystemen mit NFSv2 und NFSv3

Dies gilt speziell für NFSv3- und NFSv2-Exporte. Informationen zum Exportieren mit NFSv4 finden Sie unter Abschnitt 25.4.1, „Exportieren für NFSv4-Clients“ (S. 397).

Beim Exportieren von Dateisystemen mit NFS werden zwei Konfigurationsdateien verwendet: `/etc/exports` und `/etc/sysconfig/nfs`. Ein typischer `/etc/exports`-Dateieintrag weist folgendes Format auf:

```
/shared/directory host(list_of_options)
```

Beispiel:

```
/export 192.168.1.2(rw,sync)
```

Hier wird das Verzeichnis `/export` gemeinsam mit dem Host 192.168.1.2 mit der Optionsliste `rw,sync` verwendet. Diese IP-Adresse kann durch einen Clientnamen oder mehrere Clients mit einem Platzhalterzeichen (z. B. `*.abc.com`) oder auch durch Netzwerkgruppen ersetzt werden.

Eine detaillierte Erläuterung aller Optionen und der entsprechenden Bedeutungen finden Sie auf der man-Seite zu `exports` (`man exports`).

Starten Sie den NFS-Server nach dem Ändern von `/etc/exports` oder `/etc/sysconfig/nfs` mit dem Befehl `rcnfsserver restart` bzw. starten Sie ihn neu.

25.6 NFS mit Kerberos

Wenn die Kerberos-Authentifizierung für NFS verwendet werden soll, muss die GSS-Sicherheit aktiviert werden. Wählen Sie dazu *GSS-Sicherheit aktivieren* im ersten YaST-Dialogfeld. Zur Verwendung dieser Funktion muss ein funktionierender Kerberos-Server zur Verfügung stehen. YaST richtet diesen Server nicht ein, sondern nutzt lediglich die über den Server bereitgestellten Funktionen. Wenn Sie die Authentifizierung mittels Kerberos verwenden möchten, müssen Sie zusätzlich zur YaST-Konfiguration mindestens die nachfolgend beschriebenen Schritte ausführen, bevor Sie die NFS-Konfiguration ausführen:

1. Stellen Sie sicher, dass sich Server und Client in derselben Kerberos-Domäne befinden. Dies bedeutet, dass beide auf denselben KDC-Server (Key Distribution Center) zugreifen und die Datei `krb5.keytab` gemeinsam verwenden (der Standardspeicherort auf allen Rechnern lautet `/etc/krb5.keytab`).

2. Starten Sie den gssd-Dienst auf dem Client mit `rcgssd start`.

3 Starten Sie den svcgssd-Dienst auf dem Server mit `rcsvcgssd start`.

Weitere Informationen zum Konfigurieren eines kerberisierten NFS finden Sie über die Links in Abschnitt 25.7, „Weiterführende Informationen“ (S. 405).

25.7 Weiterführende Informationen

Genau wie für die man-Seiten zu `exports`, `nfs` und `Einhängen` stehen Informationen zum Konfigurieren eines NFS-Servers und -Clients unter `/usr/share/doc/packages/nfsidmap/README` zur Verfügung. Online-Dokumentation wird über die folgenden Web-Dokumente bereitgestellt:

- Die detaillierte technische Dokumentation finden Sie online unter SourceForge [`http://nfs.sourceforge.net/`].
- Anweisungen zum Einrichten eines kerberisierten NFS finden Sie unter NFS Version 4 Open Source Reference Implementation [`http://www.citi.umich.edu/projects/nfsv4/linux/krb5-setup.html`].
- Wenn Sie Fragen zu NFSv4 haben, lesen Sie in den Linux NFSv4-FAQ [`http://www.citi.umich.edu/projects/nfsv4/linux/faq/`] nach.

26 Dateisynchronisierung

Viele Menschen benutzen heutzutage mehrere Computer: einen Computer zu Hause, einen oder mehrere Computer am Arbeitsplatz und eventuell ein Notebook oder einen PDA für unterwegs. Viele Dateien werden auf allen diesen Computern benötigt. Da Sie mit allen Computern arbeiten und die Dateien ändern möchten, sollten alle Daten überall in aktueller Version zur Verfügung stehen.

26.1 Verfügbare Software zur Datensynchronisierung

Auf Computern, die ständig miteinander über ein schnelles Netzwerk in Verbindung stehen, ist die Datensynchronisierung kein Problem. In diesem Fall wählen Sie ein Netzwerkdateisystem, wie zum Beispiel NFS, und speichern die Dateien auf einem Server. Alle Rechner greifen dabei über das Netzwerk auf ein und dieselben Daten zu. Dieser Ansatz ist unmöglich, wenn die Netzverbindung schlecht oder teilweise gar nicht vorhanden ist. Wer mit einem Laptop unterwegs ist, ist darauf angewiesen, von allen benötigten Dateien Kopien auf der lokalen Festplatte zu haben. Wenn Dateien bearbeitet werden, stellt sich aber schnell das Problem der Synchronisierung. Wenn Sie eine Datei auf einem Computer ändern, stellen Sie sicher, dass die Kopie der Datei auf allen anderen Computern aktualisiert wird. Dies kann bei gelegentlichen Kopiervorgängen manuell mithilfe von scp oder rsync erledigt werden. Bei vielen Dateien wird das jedoch schnell aufwändig und erfordert hohe Aufmerksamkeit vom Benutzer, um Fehler, wie etwa das Überschreiben einer neuen mit einer alten Datei, zu vermeiden.

WARNUNG: Risiko des Datenverlusts

Bevor Sie Ihre Daten mit einem Synchronisierungssystem verwalten, sollten Sie mit dem verwendeten Programm vertraut sein und dessen Funktionalität testen. Für wichtige Dateien ist das Anlegen einer Sicherungskopie unerlässlich.

Zur Vermeidung der zeitraubenden und fehlerträchtigen manuellen Arbeit bei der Datensynchronisierung gibt es Programme, die diese Aufgabe mit verschiedenen Ansätzen automatisieren. Die folgenden Zusammenfassungen sollen dem Benutzer eine Vorstellung davon liefern, wie diese Programme funktionieren und genutzt werden können. Vor dem tatsächlichen Einsatz sollten Sie die Programmdokumentation sorgfältig lesen.

26.1.1 CVS

CVS, das meistens zur Versionsverwaltung von Quelltexten von Programmen benutzt wird, bietet die Möglichkeit, Kopien der Dateien auf mehreren Computern zu führen. Damit eignet es sich auch für die Datensynchronisierung. CVS führt ein zentrales Repository auf dem Server, das nicht nur die Dateien, sondern auch die Änderungen an ihnen speichert. Lokal erfolgte Änderungen werden an das Repository übermittelt und können von anderen Computern durch ein Update abgerufen werden. Beide Prozeduren müssen vom Benutzer initiiert werden.

Dabei ist CVS bei gleichzeitigen Änderungen einer Datei auf mehreren Computern sehr fehlertolerant. Die Änderungen werden zusammengeführt und nur, wenn in gleichen Zeilen Änderungen stattfanden, gibt es einen Konflikt. Die Datenbank bleibt im Konfliktfall in einem konsistenten Zustand. Der Konflikt ist nur am Client-Host sichtbar und muss dort gelöst werden.

26.1.2 rsync

Wenn Sie keine Versionskontrolle benötigen, aber große Dateistrukturen über langsame Netzwerkverbindungen synchronisieren möchten, bietet das Tool rsync ausgefeilte Mechanismen an, um ausschließlich Änderungen an Dateien zu übertragen. Dies betrifft nicht nur Textdateien sondern auch binäre Dateien. Um die Unterschiede zwischen Dateien zu erkennen, teilt rsync die Dateien in Blöcke auf und berechnet Prüfsummen zu diesen Blöcken.

Der Aufwand beim Erkennen der Änderungen hat seinen Preis. Für den Einsatz von rsync sollten die Computer, die synchronisiert werden sollen, großzügig dimensioniert sein. RAM ist besonders wichtig.

26.2 Kriterien für die Auswahl eines Programms

Bei der Entscheidung für ein Programm müssen einige wichtige Kriterien berücksichtigt werden.

26.2.1 Client-Server oder Peer-to-Peer

Zur Verteilung von Daten sind zwei verschiedene Modelle verbreitet. Im ersten Modell gleichen alle Clients ihre Dateien mit einem zentralen Server ab. Der Server muss zumindest zeitweise von allen Clients erreichbar sein. Dieses Modell wird von CVS verwendet.

Die andere Möglichkeit ist, dass alle Hosts gleichberechtigt (als Peers) vernetzt sind und ihre Daten gegenseitig abgleichen. rsync arbeitet eigentlich im Client-Modus, kann jedoch auch als Server ausgeführt werden.

26.2.2 Portabilität

CVS und rsync sind auch für viele andere Betriebssysteme, wie verschiedene Unix- und Windows-Systeme, erhältlich.

26.2.3 Interaktiv oder automatisch

In CVS startet der Benutzer die Datensynchronisierung manuell. Dies erlaubt die genaue Kontrolle über die abzugleichenden Dateien und einen einfachen Umgang mit Konflikten. Andererseits können sich durch zu lange Synchronisierungsintervalle die Chancen für Konflikte erhöhen.

26.2.4 Konflikte: Symptome und Lösungen

Konflikte treten in CVS nur selten auf, selbst wenn mehrere Leute an einem umfangreichen Programmprojekt arbeiten. Das liegt daran, dass die Dokumente zeilenweise zusammengeführt werden. Wenn ein Konflikt auftritt, ist davon immer nur ein Client betroffen. In der Regel lassen sich Konflikte in CVS einfach lösen.

In rsync gibt es keine Konfliktbehandlung. Der Benutzer muss selbst darauf achten, dass er nicht versehentlich Dateien überschreibt, und alle etwaigen Konflikte manuell lösen. Zur Sicherheit können Sie zusätzlich ein Versionierungssystem, wie RCS, verwenden.

26.2.5 Auswählen und Hinzufügen von Dateien

In CVS müssen neue Verzeichnisse und Dateien explizit mit dem Befehl `cvs add` hinzugefügt werden. Daraus resultiert eine genauere Kontrolle über die zu synchronisierenden Dateien. Andererseits werden neue Dateien häufig übersehen, vor allem, wenn aufgrund einer großen Anzahl von Dateien die Fragezeichen in der Ausgabe von `cvs update` ignoriert werden.

26.2.6 Verlauf

CVS stellt zusätzlich die Funktion der Rekonstruktion alter Dateiversionen zur Verfügung. Bei jeder Änderung kann ein kurzer Bearbeitungsvermerk hinzugefügt werden. Damit lässt sich später die Entwicklung der Dateien aufgrund des Inhalts und der Vermerke gut nachvollziehen. Für Diplomarbeiten und Programmtexte ist dies eine wertvolle Hilfe.

26.2.7 Datenmenge und Speicherbedarf

Auf jedem der beteiligten Computer ist für alle verteilten Daten genügend Speicherplatz auf der Festplatte erforderlich. CVS benötigt zusätzlichen Speicherplatz für die Repository-Datenbank auf dem Server. Da auf dem Server auch die Datei-History gespeichert wird, ist dort deutlich mehr Speicherplatz nötig. Bei Dateien im Textformat müssen

nur geänderte Zeilen neu gespeichert werden. Bei binären Dateien wächst hingegen der Platzbedarf bei jeder Änderung um die Größe der Datei.

26.2.8 GUI

Erfahrene Benutzer führen CVS in der Regel über die Kommandozeile aus. Es sind jedoch grafische Bedienoberflächen für Linux (z. B. cervisia) und andere Betriebssysteme (z. B. wincvs) verfügbar. Viele Entwicklungswerkzeuge (z. B. kdevelop) und Texteditoren (z. B. emacs) unterstützen CVS. Die Behebung von Konflikten wird mit diesen Frontends oft sehr vereinfacht.

26.2.9 Benutzerfreundlichkeit

rsync ist einfach zu verwenden und auch für Neueinsteiger geeignet. CVS ist etwas weniger bedienerfreundlich. Benutzer sollten zu deren Verwendung das Zusammenspiel zwischen Repository und lokalen Daten verstehen. Änderungen der Daten sollten zunächst immer lokal mit dem Repository zusammengeführt werden. Hierzu wird der Befehl `cvs update` verwendet. Anschließend müssen die Daten über den Befehl cvs `commit` wieder in das Repository zurückgeschickt werden. Wenn dieser Vorgang verstanden wurde, können auch Einsteiger CVS mühelos verwenden.

26.2.10 Sicherheit vor Angriffen

Idealerweise sollten die Daten bei der Übertragung vor Abhören oder Änderungen geschützt sein. CVS und rsync lassen sich einfach über SSH (Secure Shell) benutzen und sind dann gut vor solchen Angriffen geschützt. Sie sollten CVS nicht über rsh (remote shell) ausführen. Zugriffe auf CVS mit dem Mechanismus *pserver* sind in ungeschützten Netzwerken ebenfalls nicht empfehlenswert.

26.2.11 Schutz vor Datenverlust

CVS wird schon sehr lange von vielen Entwicklern zur Verwaltung ihrer Programmprojekte benutzt und ist äußerst stabil. Durch das Speichern der Entwicklungsgeschichte bietet CVS sogar Schutz vor bestimmten Benutzerfehlern, wie irrtümliches Löschen einer Datei.

Tabelle 26.1 *Funktionen der Werkzeuge zur Dateisynchronisierung: -- = sehr schlecht, - = schlecht oder nicht verfügbar, o = mittel, + = gut, ++ = hervorragend, x = verfügbar*

	CVS	**rsync**
Client/Server	C-S	C-S
Portabilität	Lin,Un*x,Win	Lin,Un*x,Win
Interaktivität	x	x
Speed	o	+
Verursacht einen Konflikt	++	o
Dateiauswahl	Auswahl/file, dir.	Verz.
Verlauf	x	-
Speicherbedarf	--	o
GUI	o	-
Schwierigkeit	o	+
Angriffe	+ (ssh)	+(ssh)
Datenverlust	++	+

26.3 Einführung in CVS

CVS bietet sich zur Synchronisierung an, wenn einzelne Dateien häufig bearbeitet werden und in einem Dateiformat vorliegen, wie ASCII-Text oder Programmquelltext. Die Verwendung von CVS für die Synchronisierung von Daten in anderen Formaten, wie z. B. JPEG-Dateien, ist zwar möglich, führt aber schnell zu großen Datenmengen, da jede Variante einer Datei dauerhaft auf dem CVS-Server gespeichert wird. Zudem bleiben in solchen Fällen die meisten Möglichkeiten von CVS ungenutzt. Die Verwen-

dung von CVS zur Dateisynchronisierung ist nur möglich, wenn alle Arbeitsstationen auf denselben Server zugreifen können.

26.3.1 Konfigurieren eines CVS-Servers

Der *Server* ist der Ort, an dem sich alle gültigen Dateien befinden, einschließlich der neuesten Version jeder Datei. Jede stationäre Arbeitsstation kann als Server benutzt werden. Wünschenswert ist, dass die Daten des CVS-Repository in regelmäßige Backups einbezogen werden.

Beim Konigurieren eines CVS-Servers ist es sinnvoll, Benutzern über SSH Zugang zum Server zu gestatten. Wenn der Benutzer auf dem Server als `tux` bekannt ist und die CVS-Software sowohl auf dem Server als auch auf dem Client installiert ist, müssen die folgenden Umgebungsvariablen auf der Client-Seite eingerichtet sein:

```
CVS_RSH=ssh CVSROOT=tux@server:/serverdir
```

Mit dem Befehl `cvsinit` können Sie den CVS-Server von der Client-Seite aus initialisieren. Das ist nur einmal erforderlich.

Abschließend muss ein Name für die Synchronisierung festgelegt werden. Wählen oder erzeugen Sie auf dem Client ein Verzeichnis, das ausschließlich Dateien enthält, die von CVS verwaltet werden sollen (es darf auch leer sein). Der Name des Verzeichnisses ist auch der Name der Synchronisierung. In diesem Beispiel wird das Verzeichnis `synchome` genannt. Wechseln Sie in dieses Verzeichnis. Um den Synchronisationsnamen auf `synchome` zu setzen, geben Sie Folgendes ein:

```
cvs import synchome tux wilber
```

Viele Befehle von CVS erfordern einen Kommentar. Zu diesem Zweck startet CVS einen Editor (den in der Umgebungsvariable `$EDITOR` definierten, ansonsten vi). Den Aufruf des Editors können Sie umgehen, indem Sie den Kommentar bereits in der Kommandozeile eingeben, wie in folgendem Beispiel:

```
cvs import –m 'this is a test' synchome tux wilber
```

26.3.2 Verwenden von CSV

Das Synchronisierungsrepository kann jetzt mit `cvsco synchome` von allen Hosts aus gecheckt werden. Dadurch wird auf dem Client das neue Unterverzeichnis `synchome` angelegt. Um Ihre Änderungen an den Server zu übermitteln, wechseln Sie in das Verzeichnis `synchome` (oder eines seiner Unterverzeichnisse) und geben Sie `cvscommit ein`.

Standardmäßig werden alle Dateien (einschließlich Unterverzeichnisse) an den Server übermittelt. Um nur einzelne Dateien oder Verzeichnisse zu übermitteln, geben Sie diese folgendermaßen an: `cvscommit datei1 verzeichnis1`. Neue Dateien und Verzeichnisse müssen dem Repository mit einem Befehl wie `cvsadd datei1 verzeichnis1` hinzugefügt werden, bevor sie an den Server übermittelt werden. Übermitteln Sie anschließend die neu hinzugefügten Dateien und Verzeichnisse mit `cvscommit datei1 verzeichnis1`.

Wenn Sie zu einer anderen Arbeitsstation wechseln, checken Sie das Synchronisierungsrepository aus, wenn nicht bereits in einer früheren Sitzung auf demselben Arbeitsplatzrechner geschehen.

Starten Sie die Synchronisierung mit dem Server über `cvs update`. Aktualisieren Sie einzelne Dateien oder Verzeichnisse, wie in `cvs update datei1 verzeichnis1`. Den Unterschied zwischen den aktuellen Dateien und den auf dem Server gespeicherten Versionen können Sie mit dem Befehl `cvs diff` oder `cvs diff datei1 verzeichnis1` anzeigen. Mit `cvs -nq update` können Sie anzeigen, welche Dateien von einer Aktualisierung betroffen sind.

Hier sind einige der Statussymbole, die während einer Aktualisierung angezeigt werden:

U
: Die lokale Version wurde aktualisiert. Dies betrifft alle Dateien, die vom Server bereitgestellt werden und auf dem lokalen System fehlen.

M
: Die lokale Version wurde geändert. Falls Änderungen am Server erfolgt sind, war es möglich, die Unterschiede mit der lokalen Kopie zusammenzuführen.

P
: Die lokale Version wurde durch einen Patch der Server-Version aktualisiert.

C
: Die lokale Datei hat einen Konflikt mit der aktuellen Version im Repository.

?
: Die Datei existiert nicht in CVS.

Der Status `M` kennzeichnet eine lokal geänderte Datei. Entweder übermitteln Sie die lokale Kopie an den Server oder Sie entfernen die lokale Datei und führen die Aktualisierung erneut durch. In diesem Fall wird die fehlende Datei vom Server abgerufen. Wenn von verschiedenen Benutzern die gleiche Datei in derselben Zeile editiert und dann übermittelt wurde, entsteht ein Konflikt, der mit `C` gekennzeichnet wird.

Beachten Sie in diesem Fall die Konfliktmarkierungen (">>" und "<<") in der Datei und entscheiden Sie sich für eine der beiden Versionen. Da diese Aufgabe unangenehm sein kann, können Sie Ihre Änderungen verwerfen, die lokale Datei löschen und mit der Eingabe `cvsup` die aktuelle Version vom Server abrufen.

26.4 Einführung in rsync

rsync bietet sich immer dann an, wenn große Datenmengen, die sich nicht wesentlich ändern, regelmäßig übertragen werden müssen. Dies ist z. B. bei der Erstellung von Sicherungskopien häufig der Fall. Ein weiteres Einsatzgebiet sind so genannte Staging-Server. Dabei handelt es sich um Server, auf denen komplette Verzeichnisstrukturen von Webservern gespeichert werden, die regelmäßig auf den eigentlichen Webserver in einer "DMZ" gespiegelt werden.

26.4.1 Konfiguration und Betrieb

rsync lässt sich in zwei verschiedenen Modi benutzen. Zum einen kann rsync zum Archivieren oder Kopieren von Daten verwendet werden. Dazu ist auf dem Zielsystem nur eine Remote-Shell, wie z. B. SSH, erforderlich. Jedoch kann rsync auch als Daemon verwendet werden und Verzeichnisse im Netz zur Verfügung stellen.

Die grundlegende Verwendung von rsync erfordert keine besondere Konfiguration. Mit rsync ist es direkt möglich, komplette Verzeichnisse auf ein anderes System zu spiegeln. Sie können beispielsweise mit dem folgenden Befehl eine Sicherung des Home-Verzeichnisses von tux auf dem Backupserver sun anlegen:

```
rsync -baz -e ssh /home/tux/ tux@sun:backup
```

Mit dem folgenden Befehl wird das Verzeichnis zurückgespielt:

```
rsync -az -e ssh tux@sun:backup /home/tux/
```

Bis hierher unterscheidet sich die Benutzung kaum von einem normalen Kopierprogramm, wie scp.

Damit rsync seine Funktionen voll ausnutzen kann, sollte das Programm im "rsync"-Modus betrieben werden. Dazu wird auf einem der Systeme der Daemon rsyncd gestartet. Konfigurieren Sie rsync in der Datei `/etc/rsyncd.conf`. Wenn beispielsweise das Verzeichnis `/srv/ftp` über rsync zugänglich sein soll, verwenden Sie die folgende Konfiguration:

```
gid = nobody
uid = nobody
read only = true
use chroot = no
transfer logging = true
log format = %h %o %f %l %b
log file = /var/log/rsyncd.log

[FTP]
        path = /srv/ftp
        comment = An Example
```

Starten Sie anschließend rsyncd mit `rcrsyncdstart`. rsyncd kann auch automatisch beim Bootvorgang gestartet werden. Hierzu muss entweder dieser Dienst in YaST im Runlevel-Editor aktiviert oder manuell der Befehl `insservrsyncd` eingegeben werden. Alternativ kann rsyncd auch von xinetd gestartet werden. Dies empfiehlt sich aber nur bei Servern, auf denen rsyncd nicht allzu oft verwendet wird.

Im obigen Beispiel wird auch eine Protokolldatei über alle Verbindungen angelegt. Diese Datei wird unter `/var/log/rsyncd.log` abgelegt.

Dann kann die Übertragung von einem Clientsystem aus getestet werden. Das geschieht mit folgendem Befehl:

```
rsync -avz sun::FTP
```

Dieser Befehl listet alle Dateien auf, die auf dem Server im Verzeichnis `/srv/ftp` liegen. Diese Anfrage wird auch in der Protokolldatei unter `/var/log/rsyncd.log` aufgezeichnet. Um die Übertragung tatsächlich zu starten, geben Sie ein Zielverzeichnis an. Verwenden Sie `.` für das aktuelle Verzeichnis. Beispiel:

```
rsync -avz sun::FTP .
```

Standardmäßig werden bei der Synchronisierung mit rsync keine Dateien gelöscht. Wenn dies erzwungen werden soll, muss zusätzlich die Option `--delete` angegeben werden. Um sicherzustellen, dass keine neueren Dateien überschrieben werden, kann stattdessen die Option `--update` angegeben werden. Dadurch entstehende Konflikte müssen manuell aufgelöst werden.

26.5 Weiterführende Informationen

CVS

Wichtige Informationen zu CVS befinden sich auch auf der Homepage `http://www.cvshome.org`.

rsync

Wichtige Informationen zu rsync finden Sie in den man-Seiten `manrsync` und `manrsyncd.conf`. Eine technische Dokumentation zur Vorgehensweise von rsync finden Sie unter `/usr/share/doc/packages/rsync/tech_report.ps`. Aktuelles zu rsync finden Sie auf der Projekt-Website unter `http://rsync.samba.org/`.

27 Der HTTP-Server Apache

Mit einem Marktanteil von mehr als 70 % ist der Apache HTTP-Server (Apache) laut einer `http://www.netcraft.com/`-Umfrage im der weltweit am häufigsten eingesetzte Webserver. Der von Apache Software Foundation (`http://www.apache.org/`) entwickelte Apache-Server läuft auf fast allen Betriebssystemen. SUSE® Linux Enterprise Server umfasst Apache, Version 2.2. In diesem Kapitel erfahren Sie, wie Apache installiert, konfiguriert und eingerichtet wird. Sie lernen SSL, CGI und weitere Module kennen und erfahren, wie Sie bei Problemen mit dem Webserver vorgehen.

27.1 Kurzanleitung

In diesem Abschnitt erfahren Sie, wie Sie Apache in kürzester Zeit installieren und einrichten. Zur Installation und Konfiguration von Apache müssen Sie als `root`-Benutzer angemeldet sein.

27.1.1 Anforderungen

Vergewissern Sie sich, dass folgende Voraussetzungen erfüllt sind, bevor Sie den Apache-Webserver einrichten:

1. Das Netzwerk des Computers ist ordnungsgemäß konfiguriert. Weitere Informationen zu diesem Thema finden Sie unter Kapitel 17, *Grundlegendes zu Netzwerken* (S. 221).

2. Durch Synchronisierung mit einem Zeitserver ist sichergestellt, dass die Systemzeit des Computers genau ist. Die exakte Uhrzeit ist für Teile des HTTP-Protokolls nötig. Weitere Informationen zu diesem Thema finden Sie unter Kapitel 20, *Zeitsynchronisierung mit NTP* (S. 305).

3. Die neuesten Sicherheitsaktualisierungen sind installiert. Falls Sie sich nicht sicher sind, führen Sie ein YaST-Online-Update aus.

4. In der Firewall ist der Standardport des Webservers (Port 80) geöffnet. Lassen Sie dazu in SUSEFirewall2 den Service *HTTP-Server* in der externen Zone zu. Diese Konfiguration können Sie in YaST vornehmen. Weitere Informationen erhalten Sie unter Abschnitt „Configuring the Firewall with YaST“ (Kapitel 8, *Masquerading and Firewalls*, ↑*Security Guide*).

27.1.2 Installation

Apache ist in der Standardinstallation von SUSE Linux Enterprise Server nicht enthalten. Um Apache zu installieren, starten Sie YaST und wählen Sie *Software* > *Software installieren oder löschen*. Wählen Sie dann *Filter* > *Schemata* und schließlich *Web and LAM Server* unter *Serverfunktionen* aus. Bestätigen Sie die Installation der abhängigen Pakete, um den Installationsvorgang abzuschließen.

Apache wird mit einer voreingestellten Standardkonfiguration installiert, die "sofort" ausgeführt werden kann. Hierzu zählt sowohl das Multiprocessing-Modul (MPM) `apache2-prefork` als aus das Modul PHP5. Weitere Informationen zu Modulen erhalten Sie unter Abschnitt 27.4, „Installieren, Aktivieren und Konfigurieren von Modulen“ (S. 440).

27.1.3 Start

Um Apache zu starten und sicherzustellen, dass Apache automatisch bei jedem Systemstart gestartet wird, öffnen Sie YaST und wählen Sie *System* > *Systemdienste (Runlevel)* aus. Suchen Sie dann nach *apache2* und aktivieren Sie den Service. Der Webserver wird sofort gestartet. Wenn Sie Ihre Änderungen nun mit *Verlassen* speichern, wird Apache beim Systemstart automatisch in Runlevel 3 und 5 gestartet. Weitere Informationen zu den Runlevels in SUSE Linux Enterprise Server und eine Beschreibung des YaST-Runlevel-Editors finden Sie in Abschnitt 7.2.3, „Konfigurieren von Systemdiensten (Runlevel) mit YaST“ (S. 78).

Über die Shell starten Sie Apache mit dem Befehl `rcapache2 start`. Mit dem Befehl `chkconfig -a apache2` stellen Sie sicher, dass Apache beim Systemstart automatisch in Runlevel 3 und 5 gestartet wird.

Sofern Sie beim Start von Apache keine Fehlermeldungen erhalten haben, müsste der Webserver nun laufen. Starten Sie einen Webbrowser und öffnen Sie `http://localhost/`. Daraufhin wird eine Apache-Testseite angezeigt, die besagt: "Es funktioniert!". Wenn diese Seite nicht angezeigt wird, lesen Sie den Abschnitt Abschnitt 27.8, „Fehlersuche“ (S. 461).

Nachdem der Webserver nun läuft, können Sie eigene Dokumente hinzufügen, die Konfiguration an Ihre Anforderungen anpassen und weitere Module mit den benötigten Funktionen installieren.

27.2 Konfigurieren von Apache

Sie haben zwei Möglichkeiten, Apache in SUSE Linux Enterprise Server zu konfigurieren: mit YaST oder manuell. Bei der manuellen Konfiguration können Sie mehr Details einstellen, allerdings müssen Sie ohne den Komfort der Bedienoberfläche von YaST zurechtkommen.

WICHTIG: Konfigurationsänderungen

Die meisten Konfigurationsänderungen werden erst nach einem Neustart bzw. nach dem Neuladen von Apache wirksam. Wenn Sie YaST zur Konfiguration verwenden und die Konfiguration mit aktiviertem *HTTP-Dienst* abschließen, wird der Rechner automatisch neu gestartet. Der manuelle Neustart wird unter Abschnitt 27.3, „Starten und Beenden von Apache“ (S. 437) beschrieben. Für die meisten Konfigurationsänderungen ist allerdings nur eine Aktualisierung mit `rcapache2 reload` erforderlich.

27.2.1 Manuelle Konfiguration von Apache

Wenn Sie den Apache-Webserver manuell konfigurieren möchten, müssen Sie die Klartext-Konfigurationsdateien als `Root`-Benutzer bearbeiten.

Konfigurationsdateien

Die Konfigurationsdateien von Apache befinden sich in zwei verschiedenen Verzeichnissen:

- `/etc/sysconfig/apache2`
- `/etc/apache2/`

/etc/sysconfig/apache2

`/etc/sysconfig/apache2` steuert einige globale Einstellungen von Apache, beispielsweise die zu ladenden Module, die einzuschließenden Konfigurationsdateien, die beim Serverstart zu verwendenden Flags sowie Flags, die der Kommandozeile hinzugefügt werden sollen. Die Konfigurationsoptionen dieser Datei sind hinreichend dokumentiert und werden daher an dieser Stelle nicht näher erläutert. Für die Konfigurationsanforderungen eines typischen Webservers dürften die Einstellungen der Datei `/etc/sysconfig/apache2` ausreichen.

/etc/apache2/

`/etc/apache2/` enthält alle Konfigurationsdateien für Apache. In diesem Abschnitt wird der Zweck jeder einzelnen Datei erklärt. Jede Datei enthält mehrere Konfigurationsoptionen (auch als *Direktiven* bezeichnet). Die Konfigurationsoptionen dieser Dateien sind hinreichend dokumentiert und werden daher an dieser Stelle nicht näher erläutert.

Die Apache-Konfigurationsdateien gliedern sich wie folgt:

```
/etc/apache2/
 |
 |- charset.conv
 |- conf.d/
 |    |
 |    |- *.conf
 |
 |- default-server.conf
 |- errors.conf
 |- httpd.conf
 |- listen.conf
 |- magic
 |- mime.types
 |- mod_*.conf
 |- server-tuning.conf
```

```
|- ssl.*
|- ssl-global.conf
|- sysconfig.d
|   |
|   |- global.conf
|   |- include.conf
|   |- loadmodule.conf . .
|
|- uid.conf
|- vhosts.d
|   |- *.conf
```

Apache-Konfigurationsdateien in /etc/apache2/

`charset.conv`
: In dieser Datei ist festgelegt, welche Zeichensätze für die verschiedenen Sprachen verwendet werden. Bearbeiten Sie diese Datei nicht.

`conf.d/*.conf`
: Dies sind Konfigurationsdateien anderer Module. Bei Bedarf können die Konfigurationsdateien in Ihre virtuellen Hostkonfigurationen eingeschlossen werden. Beispiele finden Sie in `vhosts.d/vhost.template`. Sie können damit unterschiedliche Modulsätze für verschiedene virtuelle Hosts bereitstellen.

`default-server.conf`
: Diese Datei enthält eine globale Konfiguration für virtuelle Hosts mit vernünftigen Standardeinstellungen. Statt die Werte in dieser Datei zu ändern, sollten Sie sie in der virtuellen Hostkonfiguration überschreiben.

`errors.conf`
: Diese Datei legt fest, wie Apache auf Fehler reagiert. Wenn Sie die Meldungen für alle virtuellen Hosts ändern möchten, können Sie diese Datei bearbeiten. Anderenfalls sollten Sie die entsprechenden Direktiven in den virtuellen Hostkonfigurationen überschreiben.

`httpd.conf`
: Dies ist die Hauptkonfigurationsdatei des Apache-Servers. Diese Datei sollten Sie nicht bearbeiten. Sie enthält in erster Linie Include-Anweisungen und globale Einstellungen. Globale Einstellungen können Sie in den in diesem Abschnitt aufgelisteten Konfigurationsdateien ändern. Host-spezifische Einstellungen wie DocumentRoot (absoluter Pfad) ändern Sie in der virtuellen Hostkonfiguration.

`listen.conf`
: Diese Datei bindet Apache an bestimmte IP-Adressen und Ports. Außerdem konfiguriert diese Datei das namensbasierte virtuelle Hosting (siehe „Namensbasierte virtuelle Hosts“ (S. 426)).

`magic`
: Diese Datei enthält Daten für das Modul mime_magic, mit dessen Hilfe Apache den MIME-Typ unbekannter Dateien ermittelt. Bearbeiten Sie diese Datei nicht.

`mime.types`
: Diese Datei enthält die dem System bekannten MIME-Typen (genau genommen ist diese Datei eine Verknüpfung mit `/etc/mime.types`). Bearbeiten Sie diese Datei nicht. MIME-Typen, die hier nicht aufgelistet sind, sollten Sie der Datei `mod_mime-defaults.conf` hinzufügen.

`mod_*.conf`
: Dies sind die Konfigurationsdateien der in der Standardinstallation enthaltenen Module. Weitere Informationen hierzu erhalten Sie unter Abschnitt 27.4, „Installieren, Aktivieren und Konfigurieren von Modulen“ (S. 440). Die Konfigurationsdateien optionaler Module befinden sich im Verzeichnis `conf.d`.

`server-tuning.conf`
: Diese Datei enthält Konfigurationsdirektiven für verschiedene MPMs (siehe Abschnitt 27.4.4, „Multiprocessing-Module“ (S. 445)) und allgemeine Konfigurationsoptionen, die sich auf die Leistung von Apache auswirken. Sie können diese Datei bearbeiten, sollten den Webserver anschließend aber gründlich testen.

`ssl-global.conf` und `ssl.*`
: Diese Dateien enthalten die globale SSL-Konfiguration und die SSL-Zertifikatdaten. Weitere Informationen hierzu erhalten Sie unter Abschnitt 27.6, „Einrichten eines sicheren Webservers mit SSL“ (S. 452).

`sysconfig.d/*.conf`
: Diese Konfigurationsdateien werden automatisch aus `/etc/sysconfig/apache2` generiert. Ändern Sie diese Dateien nicht. Bearbeiten Sie stattdessen die Dateien unter `/etc/sysconfig/apache2`. Fügen Sie diesem Verzeichnis auch keine weiteren Konfigurationsdateien hinzu.

`uid.conf`
: Diese Datei gibt die Benutzer- und Gruppen-ID an, unter der Apache läuft. Bearbeiten Sie diese Datei nicht.

`vhosts.d/*.conf`
: In diese Dateien sollte Ihre virtuelle Hostkonfiguration gespeichert werden. Das Verzeichnis enthält Vorlagen für virtuelle Hosts mit und ohne SSL. Jede Datei in diesem Verzeichnis mit der Erweiterung `.conf` ist automatisch Bestandteil der Apache-Konfiguration. Weitere Informationen finden Sie unter „Virtuelle Hostkonfiguration“ (S. 425).

Virtuelle Hostkonfiguration

Virtueller Host bezieht sich auf die Fähigkeit von Apache, mehrere URIs (Universal Resource Identifiers) vom gleichen physischen Computer aus bedienen zu können. Dies bedeutet, dass mehrere Domänen wie www.example.com und www.example.net von einem einzigen Webserver auf einem physischen Rechner ausgeführt werden können.

Virtuelle Hosts werden häufig eingesetzt, um Verwaltungsaufwand (nur ein Webserver muss verwaltet werden) und Hardware-Kosten (für die einzelnen Domänen ist kein dedizierter Server erforderlich) zu sparen. Virtuelle Hosts können auf Namen, IP-Adressen oder Ports basieren.

Verwenden Sie zum Auflisten aller vorhandenen virtuellen Hosts das Kommando `httpd2 -S`. Er gibt eine Liste mit dem Standardserver und allen virtuellen Hosts zusammen mit deren IP-Adressen und überwachenden Ports aus. Zusätzlich enthält die Liste einen Eintrag für jeden virtuellen Host mit dessen Speicherort in den Konfigurationsdateien.

Virtuelle Hosts können mit YaST (siehe „Virtuelle Hosts“ (S. 433)) oder manuell durch Bearbeitung einer Konfigurationsdatei konfiguriert werden. In SUSE Linux Enterprise Server ist Apache unter `/etc/apache2/vhosts.d/` standardmäßig für eine Konfigurationsdatei pro virtuellem Host vorbereitet. Alle Dateien in diesem Verzeichnis mit der Erweiterung `.conf` sind automatisch Bestandteil der Konfiguration. Außerdem enthält dieses Verzeichnis eine grundlegende Vorlage für virtuelle Hosts (`vhost.template` bzw. `vhost-ssl.template` für einen virtuellen Host mit SSL-Unterstützung).

TIPP: Erstellen Sie immer eine virtuelle Hostkonfiguration.

Es empfiehlt sich, immer eine virtuelle Hostkonfiguration zu erstellen, selbst dann, wenn der Webserver nur eine Domäne enthält. Dadurch fassen Sie nicht nur die gesamte domänenspezifische Konfiguration in einer einzigen Datei zusammen, sondern Sie können auch jederzeit auf eine funktionierende Basiskonfiguration zurückgreifen, indem Sie einfach die Konfigurationsdatei des virtuellen Hosts verschieben, löschen oder umbenennen. Aus dem gleichen Grund sollten Sie auch für jeden virtuellen Host eine eigene Konfigurationsdatei erstellen.

Der `<VirtualHost></VirtualHost>`-Block enthält die Informationen zu einer bestimmten Domäne. Wenn Apache eine Client-Anforderung für einen definierten virtuellen Host empfängt, verwendet es die in diesem Block angegebenen Direktiven. Nahezu alle Direktiven können auch im Kontext eines virtuellen Hosts verwendet werden. Weitere Informationen zu den Konfigurationsdirektiven von Apache finden Sie unter `http://httpd.apache.org/docs/2.2/mod/quickreference.html`.

Namensbasierte virtuelle Hosts

Namensbasierte virtuelle Hosts können an jeder IP-Adresse mehrere Websites bedienen. Apache verwendet das Hostfeld in dem vom Client übersandten HTTP-Header, um die Anforderung mit einem übereinstimmenden `ServerName`-Eintrag der virtuellen Hostdeklarationen zu verbinden. Wird kein übereinstimmender `ServerName` gefunden, dann wird der erste angegebene virtuelle Host als Standard verwendet.

Die Direktive `NameVirtualHost` teilt Apache mit, welche IP-Adresse (und optional welcher Port) auf Client-Anforderungen mit dem Domänennamen im HTTP-Header überwacht werden soll. Diese Option wird in der Konfigurationsdatei `/etc/apache2/listen.conf` konfiguriert.

Als erstes Argument kann der vollständig qualifizierte Domänenname eingegeben werden – empfohlen wird aber die IP-Adresse. Das zweite, optionale Argument ist der Port. Dieser ist standardmäßig Port 80 und wird mit der `Listen`-Direktive konfiguriert.

Sowohl für die IP-Adresse als auch für die Portnummer kann ein Platzhalterzeichen (`*`) eingegeben werden. In diesem Fall werden die Anforderungen an allen Schnittstellen empfangen. IPv6-Adressen müssen in eckigen Klammern eingeschlossen sein.

Beispiel 27.1 *Beispiele für namensbasierte VirtualHost-Einträge*

```
# NameVirtualHost IP-address[:Port]
NameVirtualHost 192.168.3.100:80
NameVirtualHost 192.168.3.100
NameVirtualHost *:80
NameVirtualHost *
NameVirtualHost [2002:c0a8:364::]:80
```

In einer namensbasierten virtuellen Hostkonfiguration übernimmt das `VirtualHost`-Anfangstag die zuvor unter `NameVirtualHost` deklarierte IP-Adresse (bzw. den vollständig qualifizierten Domänennamen) als Argument. Eine mit der `NameVirtualHost`-Direktive deklarierte Portnummer ist optional.

Anstelle der IP-Adresse wird auch ein Platzhalterzeichen (*) akzeptiert. Diese Syntax ist allerdings nur in Verbindung mit einem Platzhalter in `NameVirtualHost *` zulässig. IPv6-Adressen müssen in eckige Klammern eingeschlossen werden.

Beispiel 27.2 *Namensbasierte VirtualHost-Direktiven*

```
<VirtualHost 192.168.3.100:80>
  ...
</VirtualHost>

<VirtualHost 192.168.3.100>
  ...
</VirtualHost>

<VirtualHost *:80>
  ...
</VirtualHost>

<VirtualHost *>
  ...
</VirtualHost>

<VirtualHost [2002:c0a8:364::]>
  ...
</VirtualHost>
```

IP-basierte virtuelle Hosts

Bei dieser alternativen virtuellen Hostkonfiguration werden auf einem Computer mehrere IPs eingerichtet. Auf einer Apache-Instanz befinden sich mehrere Domänen, denen jeweils eine eigene IP zugewiesen ist.

Auf dem physischen Server muss für jeden IP-basierten virtuellen Host eine eigene IP-Adresse eingerichtet sein. Falls der Computer nicht über die entsprechende Anzahl an Netzwerkkarten verfügt, können auch virtuelle Netzwerkschnittstellen verwendet werden (IP-Aliasing).

Das folgende Beispiel zeigt Apache auf einem Computer mit der IP `192.168.3.100`, auf dem sich zwei Domänen mit den zusätzlichen IPs `192.168.3.101` und `192.168.3.102` befinden. Für jeden virtuellen Server wird ein eigener `VirtualHost`-Block benötigt.

Beispiel 27.3 *IP-basierte VirtualHost-Direktiven*

```
<VirtualHost 192.168.3.101>
  ...
</VirtualHost>

<VirtualHost 192.168.3.102>
  ...
</VirtualHost>
```

In diesem Beispiel sind die `VirtualHost`-Direktiven nur für Schnittstellen angegeben, die nicht `192.168.3.100` sind. Wenn für `192.168.3.100` auch eine `Listen`-Direktive konfiguriert ist, muss ein eigener IP-basierter Host eingerichtet werden, um die HTTP-Anforderungen an diese Schnittstelle zu erfüllen. Andernfalls werden die Direktiven aus der Standardserverkonfiguration (`/etc/apache2/default-server.conf`) angewendet.

Basiskonfiguration eines virtuellen Hosts

Die Konfiguration eines virtuellen Hosts sollte mindestens die folgenden Direktiven enthalten. Weitere Optionen finden Sie in `/etc/apache2/vhosts.d/vhost.template`.

`ServerName`
: Der vollständig qualifizierte Domänenname, unter dem der Host angesprochen wird.

`DocumentRoot`
: Der absolute Pfad des Verzeichnisses, aus dem Apache die Dateien für diesen Host bedient. Aus Sicherheitsgründen ist standardmäßig auf das gesamte Dateisystem

kein Zugriff möglich. Sie müssen dieses Verzeichnis daher explizit innerhalb eines `Directory`-Containers entsperren.

`ServerAdmin`
: Hier geben Sie die E-Mail-Adresse des Serveradministrators ein. Diese Adresse ist beispielsweise auf den von Apache erstellten Fehlerseiten angegeben.

`ErrorLog`
: Das Fehlerprotokoll dieses virtuellen Hosts. Ein eigenes Fehlerprotokoll für jeden virtuellen Host ist zwar nicht zwingend erforderlich, jedoch durchaus üblich, da dies die Fehlersuche erleichtert. `/var/log/apache2/` ist das Standardverzeichnis für die Protokolldateien von Apache.

`CustomLog`
: Das Zugriffsprotokoll dieses virtuellen Hosts. Ein eigenes Zugriffsprotokoll für jeden virtuellen Host ist zwar nicht zwingend erforderlich, jedoch durchaus üblich, da dies eine separate Analyse der Zugriffsdaten für jeden einzelnen Host ermöglicht. `/var/log/apache2/` ist das Standardverzeichnis für die Protokolldateien von Apache.

Wie bereits erwähnt, ist standardmäßig auf das gesamte Dateisystem kein Zugriff möglich. Die Verzeichnisse, in die Sie die Dateien gestellt haben, mit denen Apache arbeiten soll – zum Beispiel das Verzeichnis `DocumentRoot` –, müssen daher explizit entsperrt werden:

```
<Directory "/srv/www/www.example.com/htdocs">
  Order allow,deny
  Allow from all
</Directory>
```

Die vollständige Basiskonfiguration eines virtuellen Hosts sieht wie folgt aus:

Beispiel 27.4 *Basiskonfiguration eines virtuellen Hosts*

```
<VirtualHost 192.168.3.100>
  ServerName www.example.com;
  DocumentRoot /srv/www/www.example.com/htdocs
  ServerAdmin webmaster@example.com
  ErrorLog /var/log/apache2/www.example.com_log
  CustomLog /var/log/apache2/www.example.com-access_log common
  <Directory "/srv/www/www.example.com/htdocs">
    Order allow,deny
    Allow from all
  </Directory>
</VirtualHost>
```

27.2.2 Konfigurieren von Apache mit YaST

Um Ihren Webserver mit YaST zu konfigurieren, starten Sie YaST und wählen Sie *Netzwerkdienste* > *HTTP-Server* . Wenn Sie dieses Modul zum ersten Mal starten, wird der `HTTP-Server-Wizard` geöffnet. Dort müssen Sie einige administrative Einstellungen vornehmen. Nach Ausführung des Assistenten wird das unter „HTTP-Server-Konfiguration“ (S. 434) beschriebene Dialogfeld geöffnet, sobald Sie das *HTTP-Server*-Modul aufrufen.

HTTP-Server-Wizard

Der HTTP-Server-Wizard besteht aus fünf Schritten. Im letzten Schritt des Assistenten haben Sie die Möglichkeit, den Expertenkonfigurationsmodus aufzurufen, in dem Sie weitere spezielle Einstellungen vornehmen können.

Netzwerkgeräteauswahl

Geben Sie hier die Netzwerkschnittstellen und -ports an, die von Apache auf eingehende Anfragen überwacht werden. Sie können eine beliebige Kombination aus bestehenden Netzwerkschnittstellen und zugehörigen IP-Adressen auswählen. Sie können Ports aus allen drei Bereichen (Well-Known-Ports, registrierte Ports und dynamische oder private Ports) verwenden, sofern diese nicht für andere Dienste reserviert sind. Die Standardeinstellung ist die Überwachung aller Netzwerkschnittstellen (IP-Adressen) an Port 80.

Aktivieren Sie *Firewalls für gewählte Ports öffnen*, um die vom Webserver überwachten Ports in der Firewall zu öffnen. Dies ist erforderlich, um den Webserver im Netzwerk (LAN, WAN oder Internet) verfügbar zu machen. Das Schließen des Ports ist nur in Testsituationen sinnvoll, in denen kein externer Zugriff auf den Webserver erforderlich ist. Wenn Sie über mehrere Netzwerkschnittstellen verfügen, klicken Sie auf *Firewall-Details...*, um festzulegen, an welchen Schnittstellen die Ports geöffnet werden sollen.

Klicken Sie auf *Weiter*, um mit der Konfiguration fortzufahren.

Module

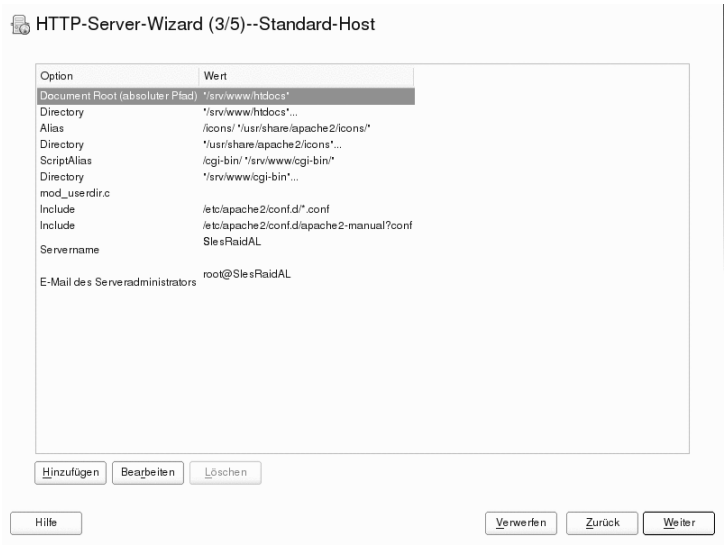
Mit der Konfigurationsoption *Module* aktivieren bzw. deaktivieren Sie die vom Webserver unterstützten Skriptsprachen. Informationen zur Aktivierung bzw. Deaktivierung anderer Module erhalten Sie unter „Servermodule“ (S. 436). Klicken Sie auf *Weiter*, um das nächste Dialogfeld zu öffnen.

Standardhost

Diese Option betrifft den Standard-Webserver. Wie in „Virtuelle Hostkonfiguration“ (S. 425) beschrieben, kann Apache von einem einzigen Computer mehrere virtuelle Hosts bedienen. Der erste in der Konfigurationsdatei deklarierte virtuelle Host wird im Allgemeinen als *Standardhost* bezeichnet. Alle nachfolgenden virtuellen Hosts übernehmen die Konfiguration des Standardhosts.

Wenn Sie die Hosteinstellungen (auch als *Direktiven* bezeichnet) bearbeiten möchten, wählen Sie den entsprechenden Eintrag in der Tabelle aus und klicken Sie auf *Bearbeiten*. Zum Hinzufügen neuer Direktiven klicken Sie auf *Hinzufügen*. Zum Löschen einer Direktive wählen Sie die Direktive aus und klicken Sie auf *Löschen*.

Abbildung 27.1 *HTTP-Server-Wizard: Standardhost*



Für den Server gelten folgende Standardeinstellungen:

`Document-Root`
: Der absolute Pfad des Verzeichnisses, aus dem Apache die Dateien für diesen Host bedient. `Dies ist standardmäßig`/srv/www/htdocs.

`Alias`

Mithilfe von `Alias`-Direktiven können URL-Adressen physischen Speicherorten im Dateisystem zugeordnet werden. Dies bedeutet, dass über eine URL sogar auf Pfade im Dateisystem außerhalb des `Document Root` zugegriffen werden kann, sofern die URL via Aliasing auf diesen Pfad verweist.

Der vorgegebene SUSE Linux Enterprise Server `Alias` für die in der Verzeichnisindex-Ansicht angezeigten Apache-Symbole, `/icons`, verweist auf `/usr/share/apache2/icons`.

`ScriptAlias`

Ähnlich wie die `Alias`-Direktive ordnet die `ScriptAlias`-Direktive eine URL einem Speicherort im Dateisystem zu. Der Unterschied besteht darin, dass `ScriptAlias` als Zielverzeichnis einen CGI-Speicherort für die Ausführung von CGI-Skripten festlegt.

`Verzeichnis`

Unter dieser `Einstellung` können Sie mehrere Konfigurationsoptionen zusammenfassen, die nur für das angegebene Verzeichnis gelten.

Hier werden auch die Zugriffs- und Anzeigeoptionen für die Verzeichnisse `/usr/share/apache2/icons` und `/srv/www/cgi-bin` konfiguriert. Eine Änderung dieser Standardeinstellungen sollte nicht erforderlich sein.

`Einbeziehen`

Hier können weitere Konfigurationsdateien hinzugefügt werden. Zwei `Include`-Direktiven sind bereits vorkonfiguriert: `/etc/apache2/conf.d/` ist das Verzeichnis für die Konfigurationsdateien externer Module. Durch diese Direktive werden alle Dateien in diesem Verzeichnis mit der Erweiterung `.conf` eingeschlossen. Durch die zweite Direktive, `/etc/apache2/conf.d/apache2-manual.conf`, wird die Konfigurationsdatei `apache2-manual` eingeschlossen.

`Servername`

Hier wird die Standard-URL festgelegt, über die Clients den Webserver kontaktieren. Verwenden Sie einen qualifizierten Domänennamen (FQDN), um den Webserver unter `http://`*`FQDN/`* zu erreichen. Alternativ können Sie auch die IP-Adresse verwenden. Sie können hier keinen willkürlichen Namen eingeben. Der Server muss unter diesem Namen "bekannt" sein.

`E-Mail des Serveradministrators`
: Hier geben Sie die E-Mail-Adresse des Serveradministrators ein. Diese Adresse ist beispielsweise auf den von Apache erstellten Fehlerseiten angegeben.

Klicken Sie am Ende der Seite *Standardhost* auf *Weiter*, um mit der Konfiguration fortzufahren.

Virtuelle Hosts

In diesem Schritt zeigt der Assistent eine Liste der bereits konfigurierten virtuellen Hosts an (siehe „Virtuelle Hostkonfiguration“ (S. 425)). Wenn Sie vor dem Starten des YaST-HTTP-Assistenten keine manuellen Änderungen vorgenommen haben, ist kein virtueller Host vorhanden.

Zum Hinzufügen eines Hosts klicken Sie auf *Hinzufügen*, um ein Dialogfeld zu öffnen, in das Sie grundlegende Informationen über den Host eingeben, z. B. *Servername*, *Übergeordnetes Verzeichnis der Server-Inhalte* (`DocumentRoot`) und *Administrator-E-Mail*. Unter *Server-Auflösung* legen Sie fest, wie der Host identifiziert wird (nach seinem Namen oder nach seiner IP-Adresse). Geben Sie den Namen oder die IP-Adresse unter *Change Virtual Host ID* (Virtuelle Host-ID ändern) an.

Klicken Sie auf *Weiter*, um mit dem zweiten Teil der virtuellen Hostkonfiguration fortzufahren.

Im zweiten Teil der virtuellen Hostkonfiguration legen Sie fest, ob CGI-Skripten zugelassen sind und welches Verzeichnis für diese Skripten verwendet wird. Dort können Sie auch SSL aktivieren. Wenn Sie SSL aktivieren, müssen Sie auch den Zertifikatpfad angeben. Informationen über SSL und Zertifikate finden Sie in Abschnitt 27.6.2, „Konfigurieren von Apache mit SSL“ (S. 458). Mit der Option *Verzeichnisindex* geben Sie an, welche Datei angezeigt wird, wenn der Client ein Verzeichnis anfordert (standardmäßig ist dies die Datei index.html). Statt der Standardeinstellung können Sie aber auch ein oder mehrere andere Dateinamen (jeweils getrennt durch ein Leerzeichen) angeben. Mit *Enable Public HTML* (Öffentliches HTML aktivieren) stellen Sie den Inhalt der öffentlichen Benutzerverzeichnisse (`~`*`user`*`/public_html/`) auf dem Server unter `http://www.example.com/~`*`user`* bereit.

WICHTIG: Erstellen virtueller Hosts

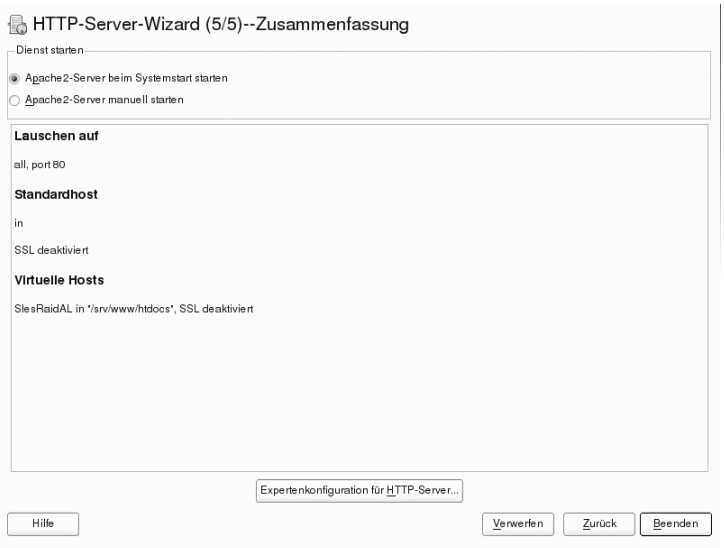
Virtuelle Hosts können Sie nicht völlig willkürlich hinzufügen. Wenn Sie namensbasierte virtuelle Hosts hinzufügen möchten, müssen die Hostnamen

im Netzwerk aufgelöst sein. Bei IP-basierten virtuellen Hosts darf jeder verfügbaren IP-Adresse nur ein Host zugewiesen sein.

Zusammenfassung

Dies ist der abschließende Schritt des Assistenten. Legen Sie hier fest, wie und wann der Apache-Server gestartet werden soll: beim Boot-Vorgang oder manuell. Außerdem erhalten Sie in diesem Schritt eine kurze Zusammenfassung Ihrer bisherigen Konfiguration. Wenn Sie mit den Einstellungen zufrieden sind, schließen Sie die Konfiguration mit *Verlassen* ab. Möchten Sie Einstellungen ändern, dann klicken Sie so oft auf *Zurück*, bis das entsprechende Dialogfeld angezeigt wird. Über *Expertenkonfiguration für HTTP-Server* können Sie hier auch das in „HTTP-Server-Konfiguration“ (S. 434) beschriebene Dialogfeld öffnen.

Abbildung 27.2 *HTTP-Server-Wizard: Zusammenfassung*



HTTP-Server-Konfiguration

Im Dialogfeld *HTTP-Server-Konfiguration* können Sie weitaus mehr Einstellungen vornehmen als im Assistenten (dieser wird ohnehin nur bei der Anfangskonfiguration des Webservers ausgeführt). Das Dialogfeld enthält vier Registerkarten, die nachfolgend beschrieben werden. Keine der in diesem Dialogfeld vorgenommenen Konfigurations-

änderungen wird sofort wirksam. Die Änderungen werden erst wirksam, wenn Sie das Dialogfeld mit *Verlassen* schließen. Klicken Sie hingegen auf *Abbrechen*, so verlassen Sie das Konfigurationsmodul und Ihre Konfigurationsänderungen werden verworfen.

Listen Ports and Addresses (Überwachte Ports und Adressen)

Geben Sie unter *HTTP-Dienst* an, ob Apache laufen soll (*Aktiviert*) oder beendet werden soll (*Deaktiviert*). Mit den Schaltflächen *Hinzufügen*, *Bearbeiten* und *Löschen* geben Sie unter *Ports überwachen* die Adressen und Ports an, die vom Server überwacht werden sollen. Standardmäßig werden alle Schnittstellen an Port 80 überwacht. Vergessen Sie nicht, das Kontrollkästchen *Firewall auf gewählten Ports öffnen* zu aktivieren. Anderenfalls wäre der Webserver von außen nicht erreichbar. Das Schließen des Ports ist nur in Testsituationen sinnvoll, in denen kein externer Zugriff auf den Webserver erforderlich ist. Wenn Sie über mehrere Netzwerkschnittstellen verfügen, klicken Sie auf *Firewall-Details...*, um festzulegen, an welchen Schnittstellen die Ports geöffnet werden sollen.

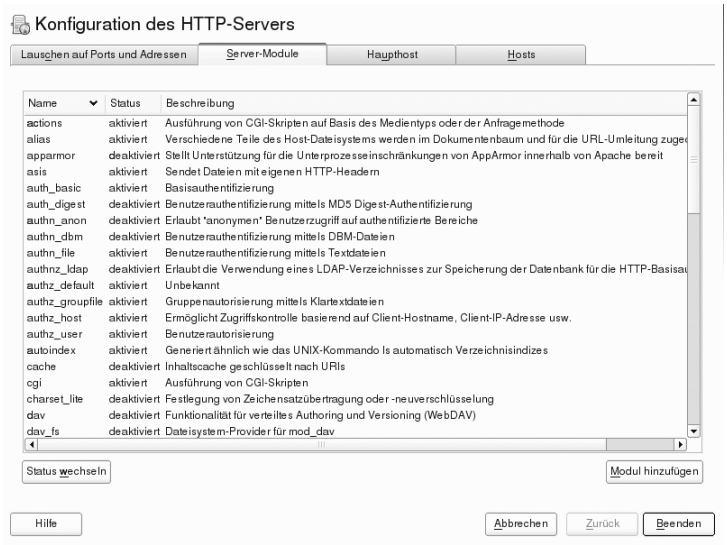
Über die Schaltfläche *Protokolldateien* können Sie das Zugriffs- oder das Fehlerprotokoll überwachen. Diese Funktion ist besonders beim Testen der Konfiguration hilfreich. Die Protokolldatei wird in einem eigenen Fenster geöffnet, aus dem Sie den Webserver auch neu starten oder neu laden können (siehe Abschnitt 27.3, „Starten und Beenden von Apache“ (S. 437)). Diese Befehle werden sofort ausgeführt.

Abbildung 27.3 *Konfiguration des HTTP-Servers: Überwachen von Ports und Adressen*

Servermodule

Über *Status wechseln* können Sie Apache2-Module aktivieren und deaktivieren. Über *Modul hinzufügen* können Sie weitere Module hinzufügen, die zwar bereits installiert, aber noch nicht in dieser Liste aufgeführt sind. Weitere Informationen über Module finden Sie in Abschnitt 27.4, „Installieren, Aktivieren und Konfigurieren von Modulen“ (S. 440).

Abbildung 27.4 *Konfiguration des HTTP-Servers: Server-Module*


Konfiguration des HTTP-Servers
Lauschen auf Ports und Adressen
Server-Module
Haupthost
Hosts
Name
Status
Beschreibung
actions aktiviert Ausführung von CGI-Skripten auf Basis des Medientyps oder der Anfragemethode
alias aktiviert Verschiedene Teile des Host-Dateisystems werden im Dokumentenbaum und für die URL-Umleitung zuge
apparmor deaktiviert Stellt Unterstützung für die Unterprozesseinschränkungen von AppArmor innerhalb von Apache bereit
asis aktiviert Sendet Dateien mit eigenen HTTP-Headern
auth_basic aktiviert Basisauthentifizierung
auth_digest deaktiviert Benutzerauthentifizierung mittels MD5 Digest-Authentifizierung
authn_anon deaktiviert Erlaubt "anonymen" Benutzerzugriff auf authentifizierte Bereiche
authn_dbm deaktiviert Benutzerauthentifizierung mittels DBM-Dateien
authn_file aktiviert Benutzerauthentifizierung mittels Textdateien
authnz_ldap deaktiviert Erlaubt die Verwendung eines LDAP-Verzeichnisses zur Speicherung der Datenbank für die HTTP-Basisau
authz_default aktiviert Unbekannt
authz_groupfile aktiviert Gruppenautorisierung mittels Klartextdateien
authz_host aktiviert Ermöglicht Zugriffskontrolle basierend auf Client-Hostname, Client-IP-Adresse usw.
authz_user aktiviert Benutzerautorisierung
autoindex aktiviert Generiert ähnlich wie das UNIX-Kommando ls automatisch Verzeichnisindizes
cache deaktiviert Inhaltscache geschlüsselt nach URIs
cgi aktiviert Ausführung von CGI-Skripten
charset_lite deaktiviert Festlegung von Zeichensatzübertragung oder -neuverschlüsselung
dav deaktiviert Funktionalität für verteiltes Authoring und Versioning (WebDAV)
dav_fs deaktiviert Dateisystem-Provider für mod_dav
Status wechseln
Modul hinzufügen
Hilfe
Abbrechen
Zurück
Beenden

Haupthost oder Hosts

Diese Dialogfelder sind mit den bereits beschriebenen identisch. in „Standardhost“ (S. 431) und „Virtuelle Hosts“ (S. 433) beschriebenen Dialogfeldern.

27.3 Starten und Beenden von Apache

Bei einer Konfiguration in YaST (siehe Abschnitt 27.2.2, „Konfigurieren von Apache mit YaST“ (S. 430)) wird Apache beim Systemstart in Runlevel 3 und 5 gestartet und in Runlevel 0, 1, 2 und 6 beendet. Dieses Verhalten können Sie im Runlevel-Editor von YaST oder mit dem Kommandozeilenprogramm `chkconfig` ändern.

Zum Starten, Beenden oder Manipulieren von Apache auf einem laufenden System verwenden Sie das init-Skript `/usr/sbin/rcapache2` (allgemeine Informationen zu init-Skripten erhalten Sie unter Abschnitt 7.2.2, „Init-Skripten“ (S. 73)). Der Befehl `rcapache2` akzeptiert folgende Parameter:

`status`
: Überprüft, ob Apache gestartet wurde.

`start`
: Startet Apache, sofern es noch nicht läuft.

`startssl`
: Startet Apache mit SSL-Unterstützung, sofern es noch nicht läuft. Weitere Informationen zu der SSL-Unterstützung finden Sie unter Abschnitt 27.6, „Einrichten eines sicheren Webservers mit SSL“ (S. 452).

`stop`
: Stoppt Apache durch Beenden des übergeordneten Prozesses.

`restart`
: Beendet Apache und startet es danach neu. Falls der Webserver noch nicht gelaufen ist, wird er nun gestartet.

`try-restart`
: Beendet Apache und startet es danach neu, sofern der Webserver bereits gelaufen ist.

`reload` oder `graceful`
: Beendet den Webserver erst, nachdem alle durch Forking erstellten Apache-Prozesse aufgefordert wurden, ihre Anforderungen vor dem Herunterfahren zu Ende zu führen. Anstelle der beendeten Prozesse werden neue Prozesse gestartet. Dies führt zu einem vollständigen "Neustart" von Apache.

TIPP

In Produktionsumgebungen ist `rcapache2 reload` die bevorzugte Methode für einen Neustart von Apache (der z. B. ausgeführt wird, damit eine Konfigurationsänderung wirksam wird). Für die Clients kommt es dabei zu keinen Verbindungsabbrüchen.

`restart-graceful`
: Startet einen zweiten Webserver, der sofort alle eingehenden Anforderungen verarbeitet. Die vorherige Instanz des Webservers wickelt weiterhin alle bestehenden Anforderungen für eine Zeitdauer ab, die mit `GracefulShutdownTimeout` definiert wurde.

  `rcapache2 restart-graceful` ist beim Upgrade auf eine neue Version oder nach dem Ändern von Konfigurationsoptionen nützlich, die einen Neustart

erfordern. Die Verwendung dieser Option sorgt für eine minimale Serverabschaltdauer.

`GracefulShutdownTimeout` muss festgelegt werden, andernfalls veranlasst `restart-graceful` einen regulären Neustart. Bei der Einstellung auf Null wartet der Server auf unbestimmte Zeit, bis alle verbleibenden Anforderungen vollständig verarbeitet sind.

Ein ordnungsgemäßer Start kann fehlschlagen, wenn die originale Apache-Instanz nicht alle nötigen Ressourcen löschen kann. In diesem Fall veranlasst das Kommando einen ordnungsgemäßen Stopp.

`stop-graceful`
Hält den Webserver nach einer Zeitdauer an, die mit `GracefulShutdownTimeout` konfiguriert wurde, um sicherzustellen, dass die bestehenden Anforderungen abgeschlossen werden können.

`GracefulShutdownTimeout` muss festgelegt sein, andernfalls verursacht `stop-graceful` einen ordnungsgemäßen Neustart. Bei der Einstellung auf Null wartet der Server auf unbestimmte Zeit, bis alle verbleibenden Anforderungen vollständig verarbeitet sind.

`configtest` oder `extreme-configtest`
Überprüft die Syntax der Konfigurationsdateien, ohne den laufenden Webserver zu beeinträchtigen. Da dieser Test beim Starten, Neuladen oder Neustarten des Servers automatisch durchgeführt wird, ist eine explizite Ausführung des Tests in der Regel nicht notwendig (bei einem Konfigurationsfehler wird der Webserver ohnehin nicht gestartet, neu geladen oder neu gestartet). Mithilfe der Option `extreme-configtest` wird der Webserver unter dem Benutzernamen `nobody` gestartet und die Konfiguration wird geladen, sodass mehr Fehler gefunden werden können. Beachten Sie, dass die SSL-Einrichtung nicht getestet werden kann, obwohl die Konfiguration geladen wurde, da SSL-Zertifikate nicht von `nobody` gelesen werden können.

`probe`
Überprüft, ob ein Neuladen des Webservers erforderlich ist (d. h., ob sich die Konfiguration geändert hat), und schlägt die erforderlichen Argumente für den Befehl `rcapache2` vor.

`server-status und full-server-status`
: Erstellt einen Dump des kurzen oder vollständigen Statusfensters. Zur Ausführung des rcapache2-Befehls mit diesem Parameter muss entweder lynx oder w3m installiert sein und das mod_status-Modul muss aktiviert sein. Außerdem muss `/etc/sysconfig/apache2` unter `APACHE_SERVER_FLAGS` das Flag `status` enthalten.

TIPP: Weitere Flags

Weitere Flags, die Sie mit dem Befehl `rcapache2` angeben, werden direkt an den Webserver weitergeleitet.

27.4 Installieren, Aktivieren und Konfigurieren von Modulen

Die Apache-Software ist modular aufgebaut. Alle Funktionen außer einigen Kernaufgaben werden von Modulen durchgeführt Dies geht sogar so weit, dass selbst HTTP durch ein Modul verarbeitet wird (http_core).

Apache-Module können bei der Entwicklung in die Apache-Binaries kompiliert oder während der Laufzeit dynamisch geladen werden. Informationen zum dynamischen Laden von Modulen erhalten Sie unter Abschnitt 27.4.2, „Aktivieren und Deaktivieren von Modulen“ (S. 441).

Apache-Module lassen sich in vier Kategorien einteilen:

Basismodule
: Basismodule sind standardmäßig in Apache enthalten. In Apache in SUSE Linux sind nur mod_so (zum Laden anderer Module) und http_core kompiliert. Alle anderen Module sind als gemeinsam genutzte Objekte verfügbar: Sie sind nicht in der Server-Binärdatei enthalten, sondern können zur Laufzeit eingebunden werden.

Erweiterungsmodule
: Im Allgemeinen sind Erweiterungsmodule im Apache-Softwarepaket enthalten, jedoch nicht statisch im Server kompiliert. In SUSE Linux Enterprise Server stehen diese Module als gemeinsame Objekte zur Verfügung, die während der Laufzeit in Apache geladen werden können.

Externe Module
: Externe Module sind nicht in der offiziellen Apache-Distribution enthalten. SUSE Linux Enterprise Server bietet jedoch einige externe Module an, die ohne großen Aufwand sofort verwendet werden können.

Multiprocessing-Module
: Multiprocessing-Module (MPMs) sind dafür verantwortlich, Anforderungen an den Webserver anzunehmen und zu verarbeiten, und stellen damit das Kernstück der Webserver-Software dar.

27.4.1 Installieren von Modulen

Wenn Sie das Standardinstallationsverfahren für Apache durchgeführt haben (siehe Abschnitt 27.1.2, „Installation“ (S. 420)), wird Apache mit allen Basis- und Erweiterungsmodulen sowie dem Multiprocessing-Modul Prefork und den externen Modulen mod_php5 und mod_python installiert.

Sie können weitere externe Module installieren. Starten Sie dazu YaST und wählen Sie *Software* > *Software installieren oder löschen*. Wählen Sie danach *Filter* > *Suche* und suchen Sie nach *apache*. Die Ergebnisliste zeigt nun neben anderen Paketen alle verfügbaren externen Apache-Module an.

27.4.2 Aktivieren und Deaktivieren von Modulen

In YaST können Sie die Skriptsprachenmodule (PHP5, Perl, Python) mit der im Abschnitt „HTTP-Server-Wizard“ (S. 430) beschriebenen Modulkonfiguration aktivieren oder deaktivieren. Alle anderen Module werden, wie im Abschnitt „Servermodule“ (S. 436) beschrieben, aktiviert oder deaktiviert.

Manuell können Sie die Module mit den Befehlen `a2enmod` *`mod_foo`* oder `a2dismod` *`mod_foo`* aktivieren bzw. deaktivieren. `a2enmod -l` gibt eine Liste aller zurzeit aktiven Module aus.

WICHTIG: Einschließen der Konfigurationsdateien externer Module

Wenn Sie externe Module manuell aktivieren, müssen Sie sicherstellen, dass auch ihre Konfigurationsdateien in allen virtuellen Hostkonfigurationen geladen werden. Die Konfigurationsdateien externer Module befinden sich im Verzeichnis `/etc/apache2/conf.d/` und werden standardmäßig nicht geladen. Wenn Sie auf allen virtuellen Hosts die gleichen Module benötigen, können Sie die Konfigurationsdateien aus diesem Verzeichnis mit `*.conf` einschließen. Anderenfalls müssen Sie die Dateien einzeln einschließen. Beispiele hierzu finden Sie in der Datei `/etc/apache2/vhosts.d/vhost.template`.

27.4.3 Basis- und Erweiterungsmodule

Alle Basis- und Erweiterungsmodule werden ausführlich in der Apache-Dokumentation beschrieben. An dieser Stelle gehen wir daher nur kurz auf die wichtigsten Module ein. Informationen zu den einzelnen Modulen erhalten Sie auch unter `http://httpd.apache.org/docs/2.2/mod/`.

mod_actions
: Bietet Methoden zur Ausführung eines Skripts, wenn ein bestimmter MIME-Typ (z. B. `application/pdf`), eine Datei mit einer bestimmten Erweiterung (z. B. `.rpm`) oder eine bestimmte Anforderungsmethode (z. B. `GET`) verlangt wird. Dieses Modul ist standardmäßig aktiviert.

mod_alias
: Dieses Modul stellt die Direktiven `Alias` und `Redirect` bereit. Damit können Sie eine URI einem bestimmten Verzeichnis zuordnen (`Alias`) bzw. eine angeforderte URL umleiten. Dieses Modul ist standardmäßig aktiviert.

mod_auth*
: Die Authentifizierungsmodule bieten verschiedene Methoden zur Authentifzierung: grundlegende Authentifzierung mit mod_auth_basic oder Digest-Authentifizierung mit mod_auth_digest. Die Digest-Authentifizierung in Apache 2.2 befindet sich noch im Versuchsstadium.

  mod_auth_basic und mod_auth_digest müssen gemeinsam mit einem Authentifizierungsanbietermodul mod_authn_* (z. B. mod_authn_file für die Authentifizierung

auf Basis einer Textdatei) und einem Autorisierungsmodul mod_authz_* (z. B. mod_authz_user für die Benutzerautorisierung) verwendet werden.

Weitere Informationen zu diesem Thema erhalten Sie im Artikel "Gewusst wie: Authentifizierung" unter `http://httpd.apache.org/docs/2.2/howto/auth.html`.

mod_autoindex
: Wenn keine Indexdatei vorhanden ist (z. B. `index.html`), generiert mod_autoindex Verzeichnislisten. Das Aussehen dieser Indizes kann konfiguriert werden. Dieses Modul ist standardmäßig aktiviert. Verzeichnislisten sind jedoch durch die `Options`-Direktive standardmäßig deaktiviert. Sie müssen diese Einstellung daher in Ihrer virtuellen Hostkonfiguration ändern. Die Standardkonfigurationsdatei dieses Moduls befindet sich unter `/etc/apache2/` und heißt mod_autoindex-defaults.conf.

mod_cgi
: mod_cgi wird zur Ausführung von CGI-Skripten benötigt. Dieses Modul ist standardmäßig aktiviert.

mod_deflate
: Mit diesem Modul kann Apache so konfiguriert werden, dass bestimmte Dateitypen automatisch vor der Bereitstellung komprimiert werden.

mod_dir
: mod_dir stellt die `DirectoryIndex`-Direktive bereit, mit der Sie festlegen können, welche Dateien bei Anforderung eines Verzeichnisses automatisch zurückgegeben werden (standardmäßig `index.html)`. Außerdem leitet dieses Modul automatisch zur korrekten URI um, wenn in einer Verzeichnisanforderung der nachgestellte Schrägstrich fehlt. Dieses Modul ist standardmäßig aktiviert.

mod_env
: Steuert die Umgebungsvariablen, die an CGI-Skripten oder SSI-Seiten übergeben werden. Sie können Umgebungsvariablen festlegen oder aufheben oder von der Shell übergeben, die den httpd-Prozess aufgerufen hat. Dieses Modul ist standardmäßig aktiviert.

mod_expires
: Mit mod_expires legen Sie fest, wie häufig Ihre Dokumente über Proxy- und Browser-Caches durch Zustellung eines `Expires`-Header aktualisiert werden. Dieses Modul ist standardmäßig aktiviert.

mod_include
: mod_include ermöglicht die Verwendung von serverseitigen Includes (SSI), die die grundlegende Funktionalität für die dynamische Generierung von HTML-Seiten bereitstellen. Dieses Modul ist standardmäßig aktiviert.

mod_info
: Dieses Modul stellt unter http://localhost/server-info/ eine umfassende Übersicht über die Serverkonfiguration bereit. Aus Sicherheitsgründen sollte der Zugriff auf diese URL generell eingeschränkt sein. Standardmäßig erhält nur `localhost` Zugriff auf diese URL. mod_info wird in der Datei `/etc/apache2/mod_info.conf` konfiguriert.

mod_log_config
: Mit diesem Modul konfigurieren Sie den Aufbau der Apache-Protokolldateien. Dieses Modul ist standardmäßig aktiviert.

mod_mime
: Dieses Modul sorgt dafür, dass eine Datei auf Basis seiner Dateinamenerweiterung mit dem korrekten MIME-Header bereitgestellt wird (z. B. `text/html` für HTML-Dokumente). Dieses Modul ist standardmäßig aktiviert.

mod_negotiation
: Dieses Modul ist für die Inhaltsverhandlung erforderlich. Weitere Informationen erhalten Sie unter `http://httpd.apache.org/docs/2.2/content-negotiation.html`. Dieses Modul ist standardmäßig aktiviert.

mod_rewrite
: Dieses Modul stellt die gleiche Funktionalität wie mod_alias bereit, bietet aber mehr Funktionen und ist somit flexibler. Mit mod_rewrite können Sie URLs auf Basis verschiedener Regeln umleiten, Header anfordern und einiges mehr.

mod_setenvif
: Legt Umgebungsvariablen auf der Basis von Details aus der Client-Anforderung fest, z. B. die Browserzeichenfolge, die der Client sendet, oder die IP-Adresse des Clients. Dieses Modul ist standardmäßig aktiviert.

mod_speling
: mod_speling versucht, typografische Fehler in URLs, beispielsweise die Groß-/Kleinschreibung, automatisch zu korrigieren.

mod_ssl
: Dieses Modul ermöglicht verschlüsselte Verbindungen zwischen dem Webserver und den Clients. Weitere Informationen finden Sie in Abschnitt 27.6, „Einrichten eines sicheren Webservers mit SSL“ (S. 452). Dieses Modul ist standardmäßig aktiviert.

mod_status
: Dieses Modul stellt unter http://localhost/server-status/ Informationen über die Aktivität und Leistung des Servers bereit. Aus Sicherheitsgründen sollte der Zugriff auf diese URL generell eingeschränkt sein. Standardmäßig erhält nur `localhost` Zugriff auf diese URl. mod_status wird in der Datei `/etc/apache2/mod_status.conf` konfiguriert.

mod_suexec
: Dieses Modul ermöglicht die Ausführung von CGI-Skripten unter einem anderen Benutzer oder einer anderen Gruppe. Dieses Modul ist standardmäßig aktiviert.

mod_userdir
: Dieses Modul ermöglicht benutzerspezifische Verzeichnisse unter *~user/*. In der Konfiguration muss die `UserDir`-Direktive angegeben sein. Dieses Modul ist standardmäßig aktiviert.

27.4.4 Multiprocessing-Module

SUSE Linux Enterprise Server bietet zwei Multiprocessing-Module (MPMs) für Apache.

Prefork-MPM

Das Prefork-MPM implementiert einen Prefork-Webserver, der keine Threads verwendet. Mit diesem Modul verhält sich der Webserver, was die Handhabung von Anforderungen betrifft, ähnlich wie Apache Version 1.x: Er isoliert jede einzelne Anforderung und verarbeitet sie in einem separaten untergeordneten Prozess (Forking). Eine Beeinträchtigung aller Anforderungen durch wenige problematische Anforderungen und somit eine Sperre des Webservers lassen sich dadurch vermeiden.

Die prozessbasierte Vorgehensweise des Prefork-MPM bietet zwar Stabilität, konsumiert aber mehr Systemressourcen wie das Worker-MPM. Für UNIX-basierte Betriebssysteme gilt das Prefork-MPM als Standard-MPM.

WICHTIG: MPMs in diesem Dokument

In diesem Dokument wird davon ausgegangen, dass Apache mit dem Prefork-MPM verwendet wird.

Worker-MPM

Das Worker-MPM implementiert einen Multithread-Webserver. Ein Thread ist die "Lightweight-Version" eines Prozesses. Der Vorteil von Threads gegenüber Prozessen ist deren geringerer Ressourcenkonsum. Anstatt lediglich untergeordnete Prozesse zu erstellen (Forking), verarbeitet das Worker-MPM Anforderungen durch Threads mit Serverprozessen. Die untergeordneten Prefork-Prozesse sind auf mehrere Threads verteilt (Multithreading). Diese Ansatzweise macht den Apache-Server durch den geringeren Ressourcenkonsum leistungsfähiger als mit dem Prefork-MPM.

Ein Hauptnachteil ist die Instabilität des Worker-MPM: Ein fehlerhafter Thread kann sich auf alle Threads eines Prozesses auswirken. Im schlimmsten Fall fällt der Server dadurch aus. Besonders bei gleichzeitiger Verwendung der Common Gateway Interface (CGI) auf einem überlasteten Apache-Server kann es zu internen Serverfehlern kommen, da Threads in diesem Fall unter Umständen nicht in der Lage sind, mit den Systemressourcen zu kommunizieren. Gegen die Verwendung des Worker-MPM in Apache spricht auch die Tatsache, dass nicht alle verfügbaren Apache-Module Thread-sicher sind und daher nicht in Verbindung mit dem Worker-MPM eingesetzt werden können.

WARNUNG: Verwendung von PHP-Modulen mit MPMs

Nicht alle verfügbaren PHP-Module sind Thread-sicher. Von einer Verwendung des Worker-MPM in Verbindung mit mod_php wird daher abgeraten.

27.4.5 Externe Module

Nachfolgend finden Sie eine Liste aller externen Module, die mit SUSE Linux Enterprise Server ausgeliefert werden. Die Dokumentation zu den einzelnen Modulen finden Sie in den jeweils genannten Verzeichnissen.

mod-apparmor
: Unterstützt Apache bei der Novell AppArmor-Einschränkung auf einzelne cgi-Skripten, die von Modulen wie mod_php5 und mod_perl benutzt werden.

  Paketname: `apache2-mod_apparmor`
  Weitere Informationen:Teil „AppArmor“ (↑*Security Guide*)

mod_mono
: Mithilfe von mod_mono können Sie ASP.NET-Seiten auf Ihrem Server ausführen.

  Paketname: `apache2-mod_mono`
  Konfigurationsdatei: `/etc/apache2/conf.d/mod_mono.conf`

mod_perl
: mod_perl ermöglicht die Ausführung von Perl-Skripten in einem eingebetteten Interpreter. Durch den dauerhaften, im Server eingebetteten Interpreter lassen sich Verzögerungen durch den Start eines externen Interpreters und den Start von Perl vermeiden.

  Paketname: `apache2-mod_perl`
  Konfigurationsdatei: `/etc/apache2/conf.d/mod_perl.conf`
  Weitere Informationen: `/usr/share/doc/packages/apache2-mod_perl`

mod_php5
: PHP ist eine serverseitige, plattformübergreifende, in HTML eingebettete Skriptsprache.

  Paketname: `apache2-mod_php5`
  Konfigurationsdatei: `/etc/apache2/conf.d/php5.conf`
  Weitere Informationen: `/usr/share/doc/packages/apache2-mod_php5`

mod_python
: mod_python bettet Python in den Apache-Webserver ein. Dies bringt Ihnen einen erheblichen Leistungsgewinn und zusätzliche Flexibilität bei der Entwicklung webbasierter Anwendungen.

  Paketname: `apache2-mod_python`
  Weitere Informationen: `/usr/share/doc/packages/apache2-mod_python`

27.4.6 Kompilieren von Modulen

Apache kann von erfahrenen Benutzern durch selbst entwickelte Module erweitert werden. Für die Entwicklung eigener Apache-Module und für die Kompilierung von Drittanbieter-Modulen sind neben dem Paket `apache2-devel` auch die entsprechenden Entwicklungstools erforderlich. `apache2-devel` enthält unter anderem die `apxs2`-Tools, die zur Kompilierung von Apache-Erweiterungsmodulen erforderlich sind.

`apxs2` ermöglicht die Kompilierung und Installation von Modulen aus dem Quellcode (einschließlich der erforderlichen Änderungen an den Konfigurationsdateien). Dadurch ergeben sich *Dynamic Shared Objects* (DSOs), die während der Laufzeit in Apache geladen werden können.

Die Binaries von `apxs2` befinden sich unter `/usr/sbin`:

- `/usr/sbin/apxs2`: Für die Entwicklung von Erweiterungsmodulen, die mit allen MPMs verwendbar sind. Die Module werden im Verzeichnis `/usr/lib/apache2` installiert.
- `/usr/sbin/apxs2-prefork`: Für die Entwicklung von Prefork-MPM-Modulen geeignet. Die Module werden im Verzeichnis `/usr/lib/apache2-prefork` installiert.
- `/usr/sbin/apxs2-worker`: Für die Entwicklung von Worker-MPM-Modulen geeignet. Die Module werden im Verzeichnis `/usr/lib/apache2-worker` installiert.

Zur Installation und Aktivierung eines Moduls aus dem Quellcode verwenden Sie den Befehl `cd /Pfad/der/Modulquelle; apxs2 -cia mod_foo.c` (`-c` kompiliert das Modul, `-i` installiert es und `-a` aktiviert es). Alle weiteren Optionen von `apxs2` werden auf der Manualpage `apxs2(1)` beschrieben.

27.5 Aktivieren von CGI-Skripten

Die Common Gateway Interface (CGI) von Apache ermöglicht die dynamische Erstellung von Inhalten mit Programmen bzw. so genannten CGI-Skripten. CGI-

Skripten können in jeder beliebigen Programmiersprache geschrieben sein. In der Regel werden aber die Skriptsprachen Perl oder PHP verwendet.

Damit Apache in der Lage ist, die von CGI-Skripten erstellten Inhalte bereitzustellen, muss das Modul mod_cgi aktiviert sein. Außerdem ist mod_alias erforderlich. Beide Module sind standardmäßig aktiviert. Informationen zur Aktivierung von Modulen finden Sie unter Abschnitt 27.4.2, „Aktivieren und Deaktivieren von Modulen“ (S. 441).

WARNUNG: CGI-Sicherheit

Die Zulassung der CGI-Skriptausführung auf dem Server ist ein Sicherheitsrisiko. Weitere Informationen finden Sie in Abschnitt 27.7, „Vermeiden von Sicherheitsproblemen“ (S. 459).

27.5.1 Konfiguration in Apache

In SUSE Linux Enterprise Server ist die Ausführung von CGI-Skripten nur im Verzeichnis `/srv/www/cgi-bin/` erlaubt. Dieses Verzeichnis ist bereits für die Ausführung von CGI-Skripten konfiguriert. Wenn Sie eine virtuelle Hostkonfiguration erstellt haben (siehe „Virtuelle Hostkonfiguration“ (S. 425)) und Ihre CGI-Skripten in einem Hostspezifischen Verzeichnis ablegen möchten, müssen Sie das betreffende Verzeichnis entsperren und für CGI-Skripten konfigurieren.

Beispiel 27.5 *CGI-Konfiguration für virtuelle Hosts*

```
ScriptAlias /cgi-bin/ "/srv/www/www.example.com/cgi-bin/"❶

<Directory "/srv/www/www.example.com/cgi-bin/">
 Options +ExecCGI❷
 AddHandler cgi-script .cgi .pl❸
 Order allow,deny❹
 Allow from all
</Directory>
```

❶ Fordert Apache auf, alle Dateien in diesem Verzeichnis als CGI-Skripten zu behandeln

❷ Aktiviert die Ausführung von CGI-Skripten

❸ Fordert den Server auf, Dateien mit den Erweiterungen .pl und .cgi als CGI-Skripten zu behandeln. passen Sie diese Anweisung entsprechend Ihren Anforderungen an

❹ Die `Order`- und `Allow`-Anweisungen legen den Standardzugriffsstatus sowie die Reihenfolge fest, in der Allow- und Deny-Anweisungen ausgewertet werden. in diesem Beispiel werden "deny"-Anweisungen vor "allow"-Anweisungen ausgewertet und der Zugriff ist von jedem Ort aus möglich.

27.5.2 Ausführen eines Beispielskripten

Die CGI-Programmierung unterscheidet sich von der herkömmlichen Programmierung insoweit, als CGI-Programmen und -Skripten ein MIME-Typ-Header wie `Content-type: text/html` vorangestellt werden muss. Dieser Header wird an den Client gesendet, damit er weiß, welchen Inhaltstyp er empfängt. Darüber hinaus muss die Skriptausgabe vom Client, in der Regel einem Webbrowser, verstanden werden. In den meisten Fällen ist dies HTML, manchmal aber auch Klartext, Bilder oder Ähnliches.

Unter `/usr/share/doc/packages/apache2/test-cgi` stellt Apache ein einfaches Testskript bereit. Dieses Skript gibt den Inhalt einiger Umgebungsvariablen als Klartext aus. Wenn Sie dieses Skript ausprobieren möchten, kopieren Sie es in das Verzeichnis `/srv/www/cgi-bin/` bzw. in das Skriptverzeichnis Ihres virtuellen Hosts (`/srv/www/www.example.com/cgi-bin/`) und benennen Sie es in `test.cgi` um.

Über den Webserver zugängliche Dateien sollten dem `root`-Benutzer gehören (siehe auch Abschnitt 27.7, „Vermeiden von Sicherheitsproblemen“ (S. 459)). Da der Webserver unter einem anderen Benutzer ausgeführt wird, müssen CGI-Skripten von jedermann ausgeführt und gelesen werden können. Wechseln Sie daher in das CGI-Verzeichnis und führen Sie den Befehl `chmod 755 test.cgi` aus, um die entsprechenden Berechtigungen einzurichten.

Rufen Sie danach `http://localhost/cgi-bin/test.cgi` oder `http://www.example.com/cgi-bin/test.cgi` auf. Nun sollte der "CGI/1.0-Testskriptbericht" angezeigt werden.

27.5.3 Fehlersuche

Wenn Sie nach der Ausführung des CGI-Testskripten statt des Testskriptberichts eine Fehlermeldung erhalten, überprüfen Sie Folgendes:

CGI-Fehlerbehebung

- Haben Sie den Server nach der Konfigurationsänderung neu geladen? Überprüfen Sie dies mit `rcapache2 probe`.
- Falls Sie ein benutzerdefiniertes CGI-Verzeichnis eingerichtet haben, ist dieses richtig konfiguriert? Falls Sie sich nicht sicher sind, führen Sie das Skript im CGI-Standardverzeichnis `/srv/www/cgi-bin/` aus. Rufen Sie das Skript dazu mit `http://localhost/cgi-bin/test.cgi` auf.
- Wurden die richtigen Berechtigungen zugewiesen? Wechseln Sie in das CGI-Verzeichnis und führen Sie `ls -l test.cgi` aus. Die Befehlsausgabe sollte mit folgender Zeile beginnen:

  ```
  -rwxr-xr-x  1 root root
  ```

- Überprüfen Sie das Skript auf Programmierfehler. Wenn Sie die Datei test.cgi nicht bearbeitet haben, dürfte sie keine Programmierfehler enthalten. Falls Sie aber eigene Programme verwenden, sollten Sie diese immer auf Programmierfehler untersuchen.

27.6 Einrichten eines sicheren Webservers mit SSL

Vertrauliche Daten wie Kreditkarteninformationen sollten nur über eine sichere, verschlüsselte Verbindung mit Authentifizierung zwischen Webserver und Client übertragen werden. mod_ssl bietet mittels der Protokolle Secure Sockets Layer (SSL) und Transport Layer Security (TLS) eine sichere Verschlüsselung für die HTTP-Kommunikation zwischen einem Client und dem Webserver. Wenn Sie SSL/TSL verwenden, wird zwischen dem Webserver und dem Client eine private Verbindung eingerichtet. Die Datenintegrität bleibt dadurch gewährleistet und Client und Server können sich gegenseitig authentifizieren.

Zu diesem Zweck sendet der Server vor der Beantwortung von Anforderungen an eine URL ein SSL-Zertifikat mit Informationen, die die Identität des Servers nachweisen. Dies garantiert, dass der Server eindeutig der richtige Endpunkt der Kommunikation ist. Außerdem wird durch das Zertifikat eine verschlüsselte Verbindung zwischen dem Client und dem Server hergestellt, die sicherstellt, dass Informationen ohne das Risiko der Freigabe sensitiver Klartextinhalte übertragen werden.

mod_ssl implementiert die SSL/TSL-Protokolle nicht selbst, sondern fungiert als Schnittstelle zwischen Apache und einer SSL-Bibliothek. In SUSE Linux Enterprise Server wird die OpenSSL-Bibliothek verwendet. OpenSSL wird bei der Installation von Apache automatisch installiert.

Die Verwendung von mod_ssl in Apache erkennen Sie in URLs am Präfix `https://` (statt `http://`).

27.6.1 Erstellen eines SSL-Zertifikats

Wenn Sie SSL/TSL mit dem Webserver einsetzen möchten, müssen Sie ein SSL-Zertifikat erstellen. Dieses Zertifikat ist für die Autorisierung zwischen Webserver und Client erforderlich, damit beide Endpunkte jeweils die Identität des anderen Endpunkts überprüfen können. Zum Nachweis der Zertifikatintegrität muss das Zertifikat von einer Organisation signiert sein, der jeder der beteiligten Benutzer vertraut.

Sie können drei Zertifikatsarten erstellen: ein "Dummy"-Zertifikat, das nur zu Testzwecken verwendet wird, ein selbst signiertes Zertifikat für einen bestimmten Benutzerkreis,

der Ihnen vertraut, und ein Zertifikat, das von einer unabhängigen, öffentlich bekannten Zertifizierungsstelle (CA) signiert wurde.

Die Zertifikaterstellung besteht im Grunde nur aus zwei Schritten: Zunächst wird ein privater Schlüssel für die Zertifizierungsstelle generiert und danach wird das Serverzertifikat mit diesem Schlüssel signiert.

TIPP: Weiterführende Informationen

Weitere Informationen über das Konzept von SSL/TSL und diesbezügliche Festlegungen finden Sie unter `http://httpd.apache.org/docs/2.2/ssl/ssl_intro.html`.

Erstellen eines "Dummy"-Zertifikats

Die Erstellung eines Dummy-Zertifikats ist einfach. Rufen Sie lediglich das Skript `/usr/bin/gensslcert` auf. Dieses Skript erstellt oder überschreibt die folgenden Dateien:

- `/etc/apache2/ssl.crt/ca.crt`
- `/etc/apache2/ssl.crt/server.crt`
- `/etc/apache2/ssl.key/server.key`
- `/etc/apache2/ssl.csr/server.csr`

Außerdem wird eine Kopie der Datei `ca.crt` im Verzeichnis `/srv/www/htdocs/CA.crt` zum Herunterladen bereitgestellt.

WICHTIG

Verwenden Sie Dummy-Zertifikate niemals in Produktionsumgebungen, sondern nur zum Testen.

Erstellen eines selbst signierten Zertifikats

Wenn Sie einen sicheren Webserver für Ihr Intranet oder einen bestimmten Benutzerkreis einrichten, reicht unter Umständen ein von Ihrer eigenen Zertifizierungsstelle signiertes Zertifikat aus.

Die Erstellung eines selbst signierten Zertifikats ist ein interaktiver Vorgang, der aus neun Schritten besteht. Wechseln Sie dazu zunächst in das Verzeichnis `/usr/share/doc/packages/apache2` und führen Sie den folgenden Befehl aus: `./mkcert.sh make --no-print-directory /usr/bin/openssl /usr/sbin/custom`. Diesen Befehl sollten Sie keinesfalls außerhalb dieses Verzeichnisses ausführen. Das Programm gibt eine Reihe von Eingabeaufforderungen aus, von denen einige Benutzereingaben erfordern.

Prozedur 27.1 *Erstellen eines selbst signierten Zertifikats mit mkcert.sh*

1. `Festlegen des für Zertifikate zu verwendenden Signaturalgorithmus`

   Wählen Sie RSA aus (R, die Standardeinstellung), da einige ältere Browser Probleme mit DSA haben.

2. `Generating RSA private key for CA (1024 bit) (Privaten RSA-Schlüssel für CA (1024 Bit) erstellen)`

   Keine Eingabe erforderlich.

3. `Generating X.509 certificate signing request for CA (X.509-Zertifikatsignierungsanforderung für CA erstellen)`

   Hier erstellen Sie den DN (Distinguished Name) der Zertifizierungsstelle. Dazu müssen Sie einige Fragen, z. B. nach dem Land oder der Organisation, beantworten. Geben Sie an dieser Stelle nur gültige Daten ein. Schließlich wird alles, was Sie hier eingeben, später im Zertifikat angezeigt. Sie müssen nicht alle Fragen beantworten. Wenn eine Frage nicht auf Sie zutrifft oder Sie eine Antwort offen lassen möchten, geben Sie "." ein. Allgemeiner Name ist der Name der CA selbst. Wählen Sie einen aussagekräftigen Namen wie CA *`mein Unternehmen`*.

4 `Generating X.509 certificate for CA signed by itself (Von CA selbst signiertes X.509-Zertifikat für CA erstellen)`

Wählen Sie Zertifikatversion 3 aus (die Standardeinstellung).

5 `Generating RSA private key for SERVER (1024 bit) (Privaten RSA-Schlüssel für SERVER (1024 Bit) erstellen)`

Keine Eingabe erforderlich.

6 `Generating X.509 certificate signing request for SERVER (X.509-Zertifikatsignierungsanforderung für SERVER erstellen)`

Hier erstellen Sie den DN für den Serverschlüssel. Es werden nahezu die gleichen Fragen gestellt wie für den DN der Zertifizierungsstelle. Ihre Antworten betreffen jedoch den Webserver und müssen nicht unbedingt identisch mit den für die Zertifizierungsstelle eingegebenen Daten sein (der Server kann sich z. B. an einem anderen Standort befinden).

WICHTIG: Auswahl eines Common Name

Als Common Name (allgemeiner Name) müssen Sie hier den vollständig qualifizierten Hostnamen des sicheren Servers eingeben (z. B. www.example.com). Anderenfalls gibt der Browser beim Zugriff auf den Webserver eine Warnung mit dem Hinweis aus, dass das Zertifikat nicht mit dem Server übereinstimmt.

---

7 `Generating X.509 certificate signed by own CA (Von eigener CA signiertes X.509-Zertifikat erstellen)`

Wählen Sie Zertifikatversion 3 aus (die Standardeinstellung).

8 `Encrypting RSA private key of CA with a pass phrase for security (Privaten RSA-Schlüssel der CA aus Sicherheitsgründen mit einem Passwort verschlüsseln)`

Aus Sicherheitsgründen empfiehlt es sich, den privaten Schlüssel der Zertifizierungsstelle mit einem Passwort zu verschlüsseln. Wählen Sie daher J aus und geben Sie ein Passwort ein.

9 `Encrypting RSA private key of SERVER with a pass phrase for security (Privaten RSA-Schlüssel des SERVERS aus Sicherheitsgründen mit einem Passwort verschlüsseln)`

Wenn Sie den Serverschlüssel mit einem Passwort verschlüsseln, müssen Sie dieses Passwort bei jedem Start des Webservers eingeben. Dies macht den automatischen Start des Webservers beim Hochfahren des Computers oder einen Neustart des Webservers nahezu unmöglich. Aus diesem Grund sollten Sie diese Frage mit N beantworten. Denken Sie aber daran, dass Ihr Schlüssel in diesem Fall ungeschützt ist, und stellen Sie sicher, dass nur autorisierte Personen Zugriff auf den Schlüssel haben.

WICHTIG: Verschlüsseln des Serverschlüssels

Wenn Sie den Serverschlüssel mit einem Passwort verschlüsseln möchten, erhöhen Sie den Wert für `APACHE_TIMEOUT` in `/etc/sysconfig/apache2`. Anderenfalls bleibt Ihnen unter Umständen nicht genügend Zeit für die Eingabe des Passworts, bevor der Startversuch des Servers wegen Zeitüberschreitung abgebrochen wird.

Die Ergebnisseite des Skripts enthält eine Liste der generierten Zertifikate und Schlüssel. Die Dateien wurden allerdings nicht, wie im Skript angegeben, im lokalen Verzeichnis `conf` erstellt, sondern in den passenden Verzeichnissen unter `/etc/apache2/`.

Der letzte Schritt besteht darin, die Zertifikatdatei der Zertifizierungsstelle aus dem Verzeichnis `/etc/apache2/ssl.crt/ca.crt` in ein Verzeichnis zu kopieren, in dem die Benutzer auf die Datei zugreifen können. Aus diesem Verzeichnis können die Benutzer die Zertifizierungsstelle in ihren Webbrowsern der Liste der bekannten und vertrauenswürdigen Zertifizierungsstellen hinzufügen. Wäre die Zertifizierungsstelle nicht in dieser Liste enthalten, würde der Browser melden, dass das Zertifikat von einer unbekannten Zertifizierungsstelle ausgegeben wurde. Das neu erstellte Zertifikat ist ein Jahr lang gültig.

WICHTIG: Eigensignierte Zertifikate

Verwenden Sie selbst signierte Zertifikate nur auf einem Webserver, auf den Benutzer zugreifen, denen Sie bekannt sind und die Ihnen als Zertifizierungsstelle vertrauen. Für einen öffentlichen Online-Versand wäre ein solches Zertifikat z. B. nicht geeignet.

Anfordern eines offiziell signierten Zertifikats

Es gibt verschiedene offizielle Zertifizierungsstellen, die Ihre Zertifikate signieren. Zertifizierungsstellen sind vertrauenswürdige unabhängige Parteien. Einem Zertifikat, das durch eine solche Zertifizierungsstelle signiert wurde, kann daher voll und ganz vertraut werden. Sichere Webserver, deren Inhalte für die Öffentlichkeit bereitstehen, verfügen in der Regel über ein offiziell signiertes Zertifikat.

Die bekanntesten offiziellen Zertifizierungsstellen sind Thawte (`http://www.thawte.com/`) und Verisign (`http://www.verisign.com`). Diese und andere Zertifizierungsstellen sind bereits in Browsern kompiliert. Zertifikate, die von diesen Zertifizierungsstellen signiert wurden, werden daher von Browsern automatisch akzeptiert.

Wenn Sie ein offiziell signiertes Zertifikat anfordern, senden Sie kein Zertifikat an die Zertifizierungsstelle, sondern eine CSR (Certificate Signing Request, Zertifikatsignierungsanforderung). Zur Erstellung einer CSR rufen Sie das Skript `/usr/share/ssl/misc/CA.sh -newreq` auf.

Das Skript fragt zunächst nach dem Passwort für die Verschlüsselung der CSR. Danach müssen Sie einen Distinguished Name (DN) eingeben. Dazu müssen Sie einige Fragen, z. B. nach dem Land oder der Organisation, beantworten. Geben Sie an dieser Stelle nur gültige Daten ein. Alles, was Sie hier eingeben, wird überprüft und später im Zertifikat angezeigt. Sie müssen nicht alle Fragen beantworten. Wenn eine Frage nicht auf Sie zutrifft oder Sie eine Antwort offen lassen möchten, geben Sie "." ein. Allgemeiner Name ist der Name der CA selbst. Wählen Sie einen aussagekräftigen Namen wie CA *`Mein Unternehmen`*. Zum Schluss müssen Sie noch ein Challenge Passwort (zur Vernichtung des Zertifikats, falls der Schlüssel kompromittiert wird) und einen alternativen Unternehmensnamen eingeben.

Die CSR wird in dem Verzeichnis erstellt, aus dem Sie das Skript aufgerufen haben. Der Name der CSR-Datei lautet `newreq.pem`.

27.6.2 Konfigurieren von Apache mit SSL

Port 443 ist auf dem Webserver der Standardport für SSL- und TLS-Anforderungen. Zwischen einem "normalen" Apache-Webserver, der Port 80 überwacht, und einem SSL/TLS-aktivierten Apache-Server, der Port 443 überwacht, kommt es zu keinen Konflikten. In der Tat kann die gleiche Apache-Instanz sowohl HTTP als auch HTTPS ausführen. In der Regel verteilen separate virtuelle Hosts die Anforderungen für Port 80 und Port 443 an separate virtuelle Server.

WICHTIG: Firewall-Konfiguration

Vergessen Sie nicht, die Firewall für den SSL-aktivierten Apache-Webserver an Port 443 zu öffnen. Sie können dazu YaST verwenden (siehe Abschnitt „Configuring the Firewall with YaST“ (Kapitel 8, *Masquerading and Firewalls*, ↑*Security Guide*)).

Zur Verwendung von SSL muss SSL in der globalen Serverkonfiguration aktiviert sein. Zur Aktivierung öffnen Sie `/etc/sysconfig/apache2` in einem Editor und suchen Sie nach `APACHE_MODULES`. Fügen Sie der Modulliste "ssl" hinzu, sofern dieser Eintrag noch nicht vorhanden ist (mod_ssl ist standardmäßig aktiviert). Suchen Sie anschließend nach `APACHE_SERVER_FLAGS` und fügen Sie "SSL" hinzu. Wenn Sie sich zuvor entschieden haben, Ihr Serverzertifikat durch ein Passwort zu verschlüsseln, sollten Sie nun den Wert von `APACHE_TIMEOUT` heraufsetzen, damit Ihnen beim Start von Apache genügend Zeit für die Eingabe des Passworts bleibt. Starten Sie den Server anschließend neu, damit die Änderungen wirksam werden. Ein Neuladen des Servers reicht dazu nicht aus.

Das Verzeichnis der virtuellen Hostkonfiguration enthält die Vorlage `/etc/apache2/vhosts.d/vhost-ssl.template`. Diese enthält SSL-spezifische Direktiven, die bereits an anderer Stelle hinreichend dokumentiert sind. Informationen über die Basiskonfiguration eines virtuellen Hosts finden Sie unter „Virtuelle Hostkonfiguration“ (S. 425).

Kopieren Sie zum Starten die Vorlage zu `/etc/apache2/vhosts.d/`*`mySSL-host`*`.conf` und bearbeiten Sie diese. Es sollte ausreichen, die Werte für die folgenden Anweisungen anzupassen:

- `DocumentRoot`

- `ServerName`
- `ServerAdmin`
- `ErrorLog`
- `TransferLog`

WICHTIG: Namensbasierte virtuelle Hosts und SSL

Auf einem Server mit nur einer IP-Adresse können nicht mehrere SSL-aktivierte virtuelle Hosts laufen. Benutzer, die versuchen, eine Verbindung mit einer solchen Konfiguration herzustellen, erhalten bei jedem Besuch der URL eine Warnung mit dem Hinweis, dass das Zertifikat nicht mit dem Namen des Servers übereinstimmt. Für die Kommunikation auf Grundlage eines gültigen SSL-Zertifikats ist eine separate IP-Adresse bzw. ein separater Port für jede SSL-aktivierte Domäne erforderlich.

27.7 Vermeiden von Sicherheitsproblemen

Ein dem öffentlichen Internet ausgesetzter Webserver erfordert ständige Wartungs- und Verwaltungsarbeiten. Sicherheitsprobleme, verursacht durch die Software wie auch durch versehentliche Fehlkonfigurationen, sind kaum zu vermeiden. Im Folgenden einige Tipps zur Verbesserung der Sicherheit.

27.7.1 Stets aktuelle Software

Bei Bekanntwerden von Sicherheitsrisiken in der Apache-Software veröffentlicht SUSE sofort einen entsprechenden Sicherheitshinweis. Dieser enthält Anleitungen zur Behebung der Risiken, die möglichst frühzeitig ausgeführt werden sollten. Die Sicherheitsankündigungen von SUSE stehen unter folgenden Adressen zur Verfügung:

- **Webseite** `http://www.novell.com/linux/security/securitysupport.html`

- **Mailingliste** `http://en.opensuse.org/Communicate#Mailinglists`
- **RSS-Newsticker** `http://www.novell.com/linux/security/suse_security.xml`

27.7.2 DocumentRoot-Berechtigungen

In SUSE Linux Enterprise Server sind das `DocumentRoot`-Verzeichnis `/srv/www/htdocs` (absoluter Pfad) und das CGI-Verzeichnis `/srv/www/cgi-bin` standardmäßig dem Benutzer bzw. der Gruppe `root` zugeordnet. Diese Berechtigungen sollten nicht geändert werden. Wenn diese Verzeichnisse für alle Benutzer modifizierbar wären, könnte jeder Benutzer Dateien darin ablegen. Diese Dateien würden dann von Apache mit `wwwrun`-Berechtigungen ausgeführt werden, was wiederum dem Benutzer unbeabsichtigt Zugriff auf die Ressourcen des Dateisystems gewähren würde. Das `DocumentRoot`-Verzeichnis und die CGI-Verzeichnisse Ihrer virtuellen Hosts sollten Sie als Unterverzeichnisse im Verzeichnis `/srv/www` anlegen. Stellen Sie auch bei diesen Verzeichnissen sicher, dass die Verzeichnisse und die darin enthaltenen Dateien dem Benutzer bzw. der Gruppe `root` zugeordnet sind.

27.7.3 Zugriff auf das Dateisystem

Standardmäßig wird in `/etc/apache2/httpd.conf` der Zugriff auf das gesamte Dateisystem verweigert. Sie sollten diese Anweisungen nicht überschreiben. Stattdessen sollten Sie explizit den Zugriff auf die Verzeichnisse aktivieren, die Apache lesen muss (siehe „Basiskonfiguration eines virtuellen Hosts“ (S. 428)). Achten Sie dabei darauf, dass keine unbefugten Personen auf kritische Dateien wie Passwort- oder Systemkonfigurationsdateien zugreifen können.

27.7.4 CGI-Skripten

Interaktive Skripten in Perl, PHP, SSI oder anderen Programmiersprachen können im Prinzip jeden beliebigen Befehl ausführen und stellen damit generell ein Sicherheitsrisiko dar. Skripten, die vom Server ausgeführt werden, sollten nur aus Quellen stammen, denen der Serveradministrator vertraut. Es wird davon abgeraten, den Benutzern die

Ausführung eigener Skripten zu erlauben. Zusätzlich empfiehlt es sich, die Sicherheit aller Skripten zu überprüfen.

Es ist durchaus üblich, sich die Skriptverwaltung durch eine Einschränkung der Skriptausführung zu vereinfachen. Dabei wird die Ausführung von CGI-Skripten auf bestimmte Verzeichnisse eingeschränkt, statt sie global zuzulassen. Die Direktiven `ScriptAlias` und `Option ExecCGI` werden zur Konfiguration verwendet. In der Standardkonfiguration von SUSE Linux Enterprise Server ist es generell nicht gestattet, CGI-Skripten von jedem beliebigen Ort aus auszuführen.

Alle CGI-Skripten werden unter dem gleichen Benutzer ausgeführt. Es kann daher zu Konflikten zwischen verschiedenen Skripten kommen. Abhilfe schafft hier das Modul suEXEC, das die Ausführung von CGI-Skripten unter einem anderen Benutzer oder einer anderen Gruppe ermöglicht.

27.7.5 Benutzerverzeichnisse

Bei der Aktivierung von Benutzerverzeichnissen (mit mod_userdir oder mod_rewrite) sollten Sie unbedingt darauf achten, keine `.htaccess`-Dateien zuzulassen. Durch diese Dateien wäre es den Benutzern möglich, die Sicherheitseinstellungen zu überschreiben. Zumindest sollten Sie die Möglichkeiten des Benutzers durch die Direktive `AllowOverRide` einschränken. In SUSE Linux Enterprise Server sind `.htaccess`-Dateien standardmäßig aktiviert. Den Benutzern ist es allerdings nicht erlaubt, mit mod_userdir `Option`-Anweisungen zu überschreiben (siehe Konfigurationsdatei `/etc/apache2/mod_userdir.conf`).

27.8 Fehlersuche

Wenn sich Apache nicht starten lässt, eine Webseite nicht angezeigt werden kann oder Benutzer keine Verbindung zum Webserver herstellen können, müssen Sie die Ursache des Problems herausfinden. Im Folgenden werden einige nützliche Ressourcen vorgestellt, die Ihnen bei der Fehlersuche behilflich sein können.

An erster Stelle sei hier das Skript `rcapache2` (siehe Abschnitt 27.3, „Starten und Beenden von Apache“ (S. 437)) genannt, das sich sehr ausführlich mit Fehlern und deren Ursachen befasst und bei Problemen mit Apache wirklich hilfreich ist. Manchmal ist es eine Versuchung, die Binärdatei `/usr/sbin/httpd2` zum Starten oder Beenden

des Webservers zu verwenden. Vermeiden Sie dies aber und verwenden Sie stattdessen besser das Skript `rcapache2`. `rcapache2` gibt sogar Tipps und Hinweise zur Behebung von Konfigurationsfehlern.

An zweiter Stelle möchten wir auf die Bedeutung von Protokolldateien hinweisen. Sowohl bei geringfügigen als auch bei schwerwiegenden Fehlern sind die Protokolldateien von Apache, in erster Linie das Fehlerprotokoll, der beste Ort, um nach Fehlerursachen zu fahnden. Mit der Direktive `LogLevel` können Sie im Übrigen die Ausführlichkeit der protokollierten Meldungen einstellen. Dies ist z. B. nützlich, wenn Sie mehr Details benötigen. Standardmäßig befindet sich das Fehlerprotokoll in `/var/log/apache2/error_log`.

TIPP: Ein einfacher Test

Sie können die Apache-Protokollmeldungen mit dem Befehl `tail -F /var/log/apache2/`*`my_error_log`* überwachen. Führen Sie anschließend den Befehl `rcapache2 restart` aus. Versuchen Sie anschließend eine Verbindung mit einem Browser herzustellen und überprüfen Sie dort die Ausgabe.

Häufig wird vergessen, die Ports für Apache in der Firewall-Konfiguration des Servers zu öffnen. YaST bietet bei der Konfiguration von Apache eine eigene Option, die sich dieses speziellen Themas annimmt (siehe Abschnitt 27.2.2, „Konfigurieren von Apache mit YaST“ (S. 430)). Bei der manuellen Konfiguration von Apache können Sie die Ports für HTTP und HTTPS in der Firewall über das Firewall-Modul von YaST öffnen.

Falls sich Ihr Problem nicht mithilfe der vorgenannten Ressourcen beheben lässt, finden Sie weitere Informationen in der Apache-Fehlerdatenbank, die online unter `http://httpd.apache.org/bug_report.html` zur Verfügung steht. Sie können sich auch an die Apache-Benutzer-Community wenden, die Sie über eine Mailingliste unter `http://httpd.apache.org/userslist.html` erreichen. Des Weiteren empfehlen wir die Newsgroup `comp.infosystems.www.servers.unix`.

27.9 Weiterführende Informationen

Das Paket `apache2-doc`, das an verschiedenen Orten bereitgestellt wird, enthält das vollständige Apache-Handbuch für die lokale Installation und Referenz. Das Handbuch ist nicht in der Standardinstallation enthalten. Am schnellsten installieren Sie es mit

dem Kommando `zypper in apache2-doc`. Nach der Installation steht das Apache-Handbuch unter `http://localhost/manual/` zur Verfügung. Unter `http://httpd.apache.org/docs-2.2/` können Sie auch im Web darauf zugreifen. SUSE-spezifische Konfigurationstipps finden Sie im Verzeichnis `/usr/share/doc/packages/apache2/README.*`.

27.9.1 Apache 2.2

Eine Liste der neuen Funktionen in Apache 2.2 finden Sie unter `http://httpd.apache.org/docs/2.2/new_features_2_2.html`. Upgrade-Informationen von Version 2.0 auf Version 2.2 erhalten Sie unter `http://httpd.apache.org/docs-2.2/upgrading.html`.

27.9.2 Apache Module

Weitere Informationen zu der in Abschnitt 27.4.5, „Externe Module“ (S. 446) beschriebenen, externen Apache-Module finden Sie unter folgenden Adressen:

mod-apparmor
`http://en.opensuse.org/AppArmor`

mod_mono
`http://www.mono-project.com/Mod_mono`

mod_perl
`http://perl.apache.org/`

mod_php5
`http://www.php.net/manual/en/install.unix.apache2.php`

mod_python
`http://www.modpython.org/`

27.9.3 Entwicklung

Weitere Informationen zur Entwicklung von Apache-Modulen sowie zur Teilnahme am Apache-Webserver-Projekt finden Sie unter folgenden Adressen:

Informationen für Apache-Entwickler
`http://httpd.apache.org/dev/`

Dokumentation für Apache-Entwickler
`http://httpd.apache.org/docs/2.2/developer/`

Entwickeln von Apache-Modulen mit Perl und C
`http://www.modperl.com/`

27.9.4 Verschiedene Informationsquellen

Wenn Sie in SUSE Linux Enterprise Server Probleme mit Apache haben, werfen Sie einen Blick in die technische Informationssuche unter `http://www.novell.com/support`. Die Entstehungsgeschichte von Apache finden Sie unter `http://httpd.apache.org/ABOUT_APACHE.html`. Auf dieser Seite erfahren Sie auch, weshalb dieser Server Apache genannt wird.

Einrichten eines FTP-Servers mit YaST

28

Mithilfe des YaST-*FTP-Server*-Moduls können Sie Ihren Computer für die Funktion als FTP-Server konfigurieren. Anonyme und/oder authentifizierte Benutzer können eine Verbindung zu Ihrem Computer herstellen und, je nach Konfiguration, Dateien mit dem FTP-Protokoll hoch- und herunterladen. YaST stellt eine einheitliche Konfigurationsschnittstelle für verschiedene auf dem System installierte FTP-Server-Daemons bereit.

Das YaST-*FTP-Server*-Konfigurationsmodul kann zum Konfigurieren zweier verschiedener FTP-Server-Daemons verwendet werden: vsftpd (Very Secure FTP Daemon) und pure-ftpd. Nur installierte Server können konfiguriert werden.

Die vsftpd- und pure-ftpd-Server verfügen über leicht unterschiedliche Konfigurationsoptionen, besonders im Dialogfeld *Experteneinstellungen*. Dieses Kapitel beschreibt die Einstellungen des vsftpd-Servers.

Wenn das YaST FTP Server-Modul in Ihrem System nicht verfügbar ist, installieren Sie das Paket `yast2-ftp-server`.

Führen Sie zum Konfigurieren des FTP-Servers mit YaST die folgenden Schritte aus:

1. Öffnen Sie das YaST-Kontrollzentrum und wählen Sie *Netzwerkdienste* > *FTP-Server* oder führen Sie das Kommando `yast2 ftp-server` als `root` aus.

2. Wenn auf Ihrem System kein FTP-Server installiert ist, werden Sie gefragt, welcher Server installiert werden soll, wenn das YaST FTP Server-Modul gestartet wird. Wählen Sie einen Server aus und bestätigen Sie den Dialog.

3 Konfigurieren Sie im Dialogfeld *Start* den Startvorgang des FTP-Servers. Weitere Informationen finden Sie unter Abschnitt 28.1, „Starten des FTP-Servers“ (S. 466).

   Konfigurieren Sie im Dialogfeld *Allgemein* die FTP-Verzeichnisse, eine Begrüßung, die Masken zum Erstellen von Dateien sowie verschiedene andere Parameter. Weitere Informationen finden Sie unter Abschnitt 28.2, „Allgemeine FTP-Einstellungen“ (S. 467).

   Legen Sie im Dialogfeld *Leistung* die Parameter fest, die sich auf das Laden des FTP-Servers auswirken. Weitere Informationen finden Sie unter Abschnitt 28.3, „FTP-Leistungseinstellungen“ (S. 468).

   Legen Sie im Dialogfeld *Authentifizierung* fest, ob der FTP-Server für anonyme und/oder authentifizierte Benutzer verfügbar sein soll. Weitere Informationen finden Sie unter Abschnitt 28.4, „Authentifizierung “ (S. 469).

   Konfigurieren Sie im Dialogfeld *Einstellungen für Experten*den Betriebsmodus des FTP-Servers, der SSL-Verbindungen sowie die Firewall-Einstellungen. Weitere Informationen finden Sie unter Abschnitt 28.5, „Einstellungen für Experten“ (S. 469).

4 Klicken Sie auf *Beenden*, um die Konfigurationen zu speichern.

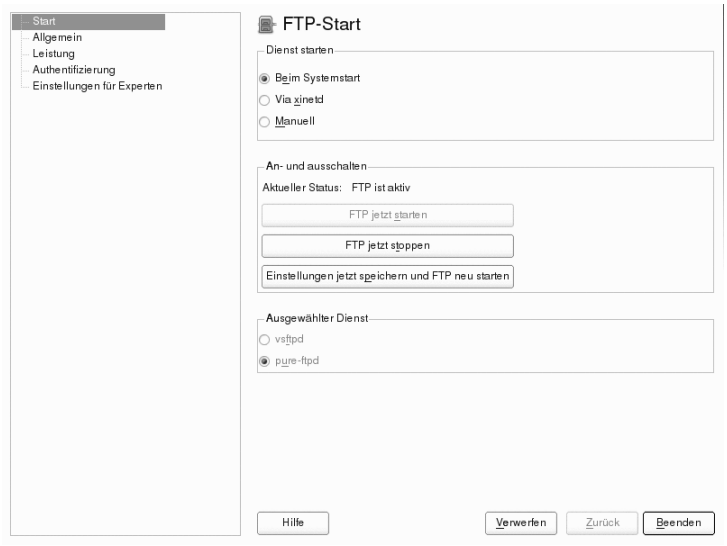
28.1 Starten des FTP-Servers

Legen Sie im Bereich *Dienststart* des Dialogfelds *FTP-Start* die Art und Weise fest, in der der FTP-Server gestartet wird. Sie können den Server entweder automatisch während des Systemstarts oder manuell starten. Wenn der FTP-Server erst bei einer FTP-Verbindungsanfrage gestartet werden soll, wählen Sie *Via xinetd* aus.

Der aktuelle Status des FTP-Servers wird im Bereich *An- und ausschalten* im Dialogfeld *FTP-Start* angezeigt. Starten Sie den FTP-Server, indem Sie auf *FTP-Server jetzt starten* klicken. Um den Server zu stoppen, klicken Sie auf *Stoppen FTP*. Nachdem Sie die Servereinstellungen geändert haben, klicken Sie auf *Einstellungen speichern und FTP jetzt neu starten*. Ihre Konfigurationen werden gespeichert, indem für das Konfigurationsmodul *Akzeptieren* beibehalten wird.

Im Bereich *Ausgewählter Dienst* des Dialogfelds *FTP-Start* wird der verwendete FTP-Server angezeigt. Entweder vsftpd (Very Secure FTP Daemon) oder pure-ftpd können verwendet werden. Wenn beide Server installiert sind, können Sie zwischen ihnen umschalten.

Abbildung 28.1 *FTP-Serverkonfiguration - Start*



28.2 Allgemeine FTP-Einstellungen

Im Bereich *Allgemeine Einstellungen* des Dialogfelds *Allgemeine FTP-Einstellungen* können Sie die *Willkommensnachricht* festlegen, die nach der Verbindungsherstellung zum FTP-Server angezeigt wird.

Wenn Sie die Option *Chroot Everyone* (Alle platzieren) aktivieren, werden alle lokalen Benutzer nach der Anmeldung in einem Chroot Jail in ihrem Home-Verzeichnis platziert Diese Option hat Auswirkungen auf die Sicherheit, besonders wenn die Benutzer über Uploadberechtigungen oder Shellzugriff verfügen, daher sollten Sie beim Aktivieren dieser Option mit Bedacht vorgehen.

Wenn Sie die Option *Ausführliche Protokollierung* aktivieren, werden alle FTP-Anfragen und -Antworten protokolliert.

Sie können die Berechtigungen für Dateien, die von anonymen und/oder authentifizierten Benutzern erstellt wurden, mit umask einschränken. Die in umask festgelegten Bits stellen die Berechtigungen dar, die immer für neu erstellte Dateien deaktiviert werden müssen. Legen Sie die Dateierstellungsmaske für anonyme Benutzer in *Umask für anonyme Benutzer* fest und die Dateierstellungsmaske für authentifizierte Benutzer in *Umask für authentifizierte Benutzer*. Die Masken sollten als Oktalzahlen mit führender Null eingegeben werden.

Legen Sie im Bereich *FTP-Verzeichnisse* die für anonyme und autorisierte Benutzer verwendeten Verzeichnisse fest. Wenn Sie auf *Durchsuchen* klicken, können Sie ein zu verwendendes Verzeichnis aus dem lokalen Dateisystem wählen. Das standardmäßige FTP-Verzeichnis für anonyme Benutzer ist `/srv/ftp`. Beachten Sie, dass vsftpd keine Verzeichnisschreibrechte für alle Benutzer erteilt. Stattdessen wird das Unterverzeichnis `upload` mit Schreibberechtigungen für anonyme Benutzer erstellt.

ANMERKUNG

Der pure-ftpd-Server ermöglicht es, dass anonyme Benutzer über Schreibberechtigungen für dieses FTP-Verzeichnis verfügen. Stellen Sie sicher, dass Sie die Schreibberechtigungen im Verzeichnis, das mit pure-ftpd verwendet wurde, entfernen, bevor Sie zum vsftpd-Server zurückschalten.

28.3 FTP-Leistungseinstellungen

Unter *FTP-Leistungseinstellungen* legen Sie die Parameter fest, die sich auf das Laden des FTP-Servers auswirken. *Max. Lerrlaufzeit* entspricht der Maximalzeit (in Minuten), die der Remote-Client zwischen FTP-Kommandos pausieren darf. Bei einer längeren Inaktivität wird die Verbindung zum Remote-Client getrennt. *Max. Clients für eine IP* bestimmt die maximale Clientanzahl, die von einer einzelnen IP-Adresse aus verbunden sein können. *Max. Clients* bestimmt die maximale Clientanzahl, die verbunden sein können. Alle zusätzlichen Clients erhalten eine Fehlermeldung.

Die maximale Datenübertragungsrate (in KB/s) wird in *Lovale Max Rate* (Lokale max. Rate) für lokale authentifizierte Benutzer und in *Anonymous Max Rate* (Anonyme max. Rate) für anonyme Benutzer festgelegt. Der Standardwert für diese Einstellung ist 0, was für eine unbegrenzte Datenübertragungsrate steht.

28.4 Authentifizierung

Im Bereich *Enable/Disable Anonymous and Local Users* (Anonyme und lokale Benutzer aktivieren/deaktivieren) des Dialogfelds *Authentifizierung* können Sie festlegen, welche Benutzer auf Ihren FTP-Server zugreifen dürfen. Sie können nur anonymen Benutzern, nur authentifizierten Benutzern mit Konten im System oder beiden Benutzertypen den Zugriff gewähren.

Wenn Sie es Benutzern ermöglichen möchten, Dateien auf den FTP-Server hochzuladen, aktivieren Sie die Option *Hochladen aktivieren* im Bereich *Hochladen* des Dialogfelds *Authentifizierung*. Hier können Sie das Hochladen und das Erstellen von Verzeichnissen sogar für anonyme Benutzer zulassen, indem Sie das entsprechende Kontrollkästchen aktivieren.

ANMERKUNG

Wenn ein vsftpd-Server verwendet wird und anonyme Benutzer Dateien hochladen oder Verzeichnisse erstellen dürfen, muss ein Unterverzeichnis mit Schreibberechtigung für alle Benutzer im anonymen FTP-Verzeichnis erstellt werden.

28.5 Einstellungen für Experten

Ein FTP-Server kann im aktiven oder passiven Modus ausgeführt werden. Standardmäßig wird der Server im passiven Modus ausgeführt. Um in den aktiven Modus zu wechseln, deaktivieren Sie einfach die Option *Passiven Modus aktivieren* im Dialogfeld *Einstellungen für Experten*. Sie können außerdem den Portbereich ändern, der auf dem Server für den Datenstrom verwendet wird, indem Sie die Optionen *Min Port für Pas.- Modus* und *Max Port für Pas.-Modus* bearbeiten.

Wenn Sie eine verschlüsselte Kommunikation zwischen den Clients und dem Server wünschen, können Sie das FTPS-Protokoll (FTP/SSH) verwenden. Beachten Sie aber, dass sich FTPS von dem häufiger verwendeten SFTP (SSH File Transport Protocol) unterscheidet. Wenn Sie das FTPS-Protokoll verwenden möchten, können Sie die SSL-Optionen im Dialogfeld *Einstellungen für Experten* festlegen.

Wenn Ihr System von einer Firewall geschützt wird, aktivieren Sie *Port in Firewall öffnen*, um eine Verbindung zum FTP-Server zu ermöglichen.

28.6 Weitere Informationen

Weitere Informationen zum vsftpd-Server finden Sie in den man-Seiten zu `pure-ftpd`, `vsftpd` und `vsftpd.conf`.

29 Der Proxyserver Squid

Squid ist ein häufig verwendeter Proxy-Cache für Linux- und UNIX-Plattformen. Das bedeutet, dass er angeforderte Internetobjekte, wie beispielsweise Daten auf einem Web- oder FTP-Server, auf einem Computer speichert, der sich näher an der Arbeitsstation befindet, die die Anforderung ausgegeben hat, als der Server. Er kann in mehreren Hierarchien eingerichtet werden. So werden optimale Reaktionszeiten und die Nutzung einer niedrigen Bandbreite garantiert – auch bei Modi, die für den Endbenutzer transparent sind. Zusätzliche Software, wie squidGuard, kann zum Filtern der Webinhalte verwendet werden.

Squid dient als Proxy-Cache. Er leitet Objektanforderungen von Clients (in diesem Fall: von Webbrowsern) an den Server weiter. Wenn die angeforderten Objekte vom Server eintreffen, stellt er die Objekte dem Client zu und behält eine Kopie davon im Festplatten-Cache. Einer der Vorteile des Cachings besteht darin, dass mehrere Clients, die dasselbe Objekt anfordern, aus dem Festplatten-Cache versorgt werden können. Dadurch können die Clients die Daten wesentlich schneller erhalten als aus dem Internet. Durch dieses Verfahren wird außerdem der Datenverkehr im Netzwerk reduziert.

Neben dem eigentlichen Caching bietet Squid eine breite Palette von Funktionen, wie die Verteilung der Last auf mehrere miteinander kommunizierende Hierarchien von Proxyservern, die Definition strenger Zugriffssteuerungslisten für alle Clients, die auf den Proxy zugreifen, das Zulassen oder Verweigern des Zugriffs auf bestimmte Webseiten mithilfe anderer Anwendungen und das Erstellen von Statistiken zu häufig besuchten Webseiten zur Bewertung der Internetgewohnheiten des Benutzers. Squid ist kein generischer Proxy. Er fungiert normalerweise nur bei HTTP-Verbindungen als Proxy. Außerdem unterstützt er die Protokolle FTP, Gopher, SSL und WAIS, nicht jedoch andere Internetprotokolle, wie Real Audio, News oder Video-Konferenzen. Da Squid nur das UDP-Protokoll für die Bereitstellung von Kommunikation zwischen

verschiedenen Caches unterstützt, werden zahlreiche andere Multimedia-Programme nicht unterstützt.

29.1 Einige Tatsachen zu Proxy-Caches

Als Proxy-Cache kann Squid auf verschiedene Weise verwendet werden. In Kombination mit einer Firewall kann er die Sicherheit unterstützen. Mehrere Proxies können gemeinsam verwendet werden. Außerdem kann er ermitteln, welche Objekttypen für wie lange im Cache gespeichert werden sollen.

29.1.1 Squid und Sicherheit

Squid kann zusammen mit einer Firewall verwendet werden, um interne Netzwerke mithilfe eines Proxy-Caches gegen Zugriffe von außen zu schützen. Die Firewall verweigert allen Clients Zugriff auf externe Dienste mit Ausnahme von Squid. Alle Webverbindungen müssen vom Proxy erstellt werden. Bei dieser Konfiguration steuert Squid den gesamten Webzugriff.

Wenn zur Firewall-Konfiguration eine DMZ gehört, sollte der Proxy in dieser Zone betrieben werden. In Abschnitt 29.5, „Konfigurieren eines transparenten Proxy“ (S. 485) wird die Implementierung eines *transparenten* Proxys beschrieben. Dadurch wird die Konfiguration der Clients erleichtert, da sie in diesem Fall keine Informationen zum Proxy benötigen.

29.1.2 Mehrere Caches

Mehrere Instanzen von Squid können für den Austausch von Objekten konfiguriert werden. Dadurch verringert sich die Gesamtlast im System und die Wahrscheinlichkeit, ein Objekt zu finden, das bereits im lokalen Netzwerk vorhanden ist, erhöht sich. Außerdem können Cache-Hierarchien konfiguriert werden. Ein Cache kann Objektanforderungen an gleichgeordnete oder übergeordnete Caches weiterleiten, sodass er Objekte aus einem anderen Cache im lokalen Netzwerk oder direkt aus der Quelle erhält.

Die Auswahl einer geeigneten Topologie für die Cache-Hierarchie ist von entscheidender Bedeutung, da es nicht erstrebenswert ist, das Gesamtaufkommen an Datenverkehr im Netzwerk zu erhöhen. Bei sehr großen Netzwerken ist es sinnvoll, einen Proxyserver für jedes Subnetzwerk zu konfigurieren und mit einem übergeordneten Proxy zu verbinden, der wiederum mit dem Proxy-Cache des ISP verbunden ist.

Diese gesamte Kommunikation wird über das ICP (Internet Cache Protocol) abgewickelt, das über dem UDP-Protokoll ausgeführt wird. Die Übertragungen zwischen den Caches erfolgen über HTTP (Hypertext Transmission Protocol) auf der Grundlage von TCP.

Um den geeignetsten Server zum Abrufen der Objekte zu finden, sendet ein Cache eine ICP-Anforderung an alle gleichgeordneten Proxies. Diese beantworten die Anforderungen über ICP-Antworten mit einem HIT-Code, wenn das Objekt erkannt wurde bzw. mit einem MISS-Code, wenn es nicht erkannt wurde. Wenn mehrere HIT-Antworten gefunden wurden, legt der Proxyserver fest, von welchem Server heruntergeladen werden soll. Diese Entscheidung ist unter anderem davon abhängig, welcher Cache die schnellste Antwort gesendet hat bzw. welcher näher ist. Wenn keine zufrieden stellenden Antworten eingehen, wird die Anforderung an den übergeordneten Cache gesendet.

TIPP

Um eine Verdopplung der Objekte in verschiedenen Caches im Netzwerk zu vermeiden, werden andere ICP-Protokolle verwendet, wie beispielsweise CARP (Cache Array Routing Protocol) oder HTCP (Hypertext Cache Protocol). Je mehr Objekte sich im Netzwerk befinden, desto größer ist die Wahrscheinlichkeit, das gewünschte zu finden.

29.1.3 Caching von Internetobjekten

Nicht alle im Netzwerk verfügbaren Objekte sind statisch. Es gibt eine Vielzahl dynamisch erstellter CGI-Seiten, Besucherzähler und verschlüsselter SSL-Inhaltsdokumente. Derartige Objekte werden nicht im Cache gespeichert, da sie sich bei jedem Zugriff ändern.

Es bleibt die Frage, wie lange alle anderen im Cache gespeicherten Objekte dort verbleiben sollten. Um dies zu ermitteln, wird allen Objekten im Cache einer von mehreren möglichen Zuständen zugewiesen. Web- und Proxyserver ermitteln den Status eines Objekts, indem sie Header zu diesen Objekten hinzufügen, beispielsweise "Zuletzt

geändert" oder "Läuft ab", und das entsprechende Datum. Andere Header, die angeben, dass Objekte nicht im Cache gespeichert werden dürfen, werden ebenfalls verwendet.

Objekte im Cache werden normalerweise aufgrund mangelnden Festplattenspeichers ersetzt. Dazu werden Algorithmen, wie beispielsweise LRU (last recently used), verwendet. Dies bedeutet im Wesentlichen, dass der Proxy die Objekte löscht, die am längsten nicht mehr angefordert wurden.

29.2 Systemvoraussetzungen

Die wichtigste Aufgabe besteht darin, die maximale Netzwerklast zu ermitteln, die das System tragen muss. Daher muss besonders auf die Belastungsspitzen geachtet werden, die mehr als das Vierfache des Tagesdurchschnitts betragen können. Im Zweifelsfall ist es vorzuziehen, die Systemanforderungen zu hoch einzuschätzen, da es zu erheblichen Einbußen in der Qualität des Diensts führen kann, wenn Squid an der Grenze seiner Leistungsfähigkeit arbeitet. Die folgenden Abschnitte widmen sich den einzelnen Systemfaktoren in der Reihenfolge ihrer Wichtigkeit.

29.2.1 Festplatten

Da Geschwindigkeit beim Caching eine wichtige Rolle spielt, muss diesem Faktor besondere Aufmerksamkeit gewidmet werden. Bei Festplatten wird dieser Parameter als *random seek time* (Zufallszugriffszeit, gemessen in Millisekunden) beschrieben. Da die Datenblöcke, die Squid von der Festplatte liest oder auf die Festplatte schreibt, eher klein zu sein scheinen, ist die Zugriffszeit der Festplatte entscheidender als ihr Datendurchsatz. Für die Zwecke von Proxies sind Festplatten mit hoher Rotationsgeschwindigkeit wohl die bessere Wahl, da bei diesen der Lese-Schreib-Kopf schneller an die gewünschte Stelle gebracht werden kann. Eine Möglichkeit zur Systembeschleunigung besteht in der gleichzeitigen Verwendung mehrerer Festplatten oder im Einsatz von Striping-RAID-Arrays.

29.2.2 Größe des Festplatten-Cache

Bei einem kleinen Cache ist die Wahrscheinlichkeit eines HIT (Auffinden des angeforderten Objekts, das sich bereits dort befindet) gering, da der Cache schnell voll ist und die weniger häufig angeforderten Objekte durch neuere ersetzt werden. Wenn beispiels-

weise 1 GB für den Cache zur Verfügung steht und die Benutzer nur Datenverkehr im Umfang von 10 MB pro Tag in Anspruch nehmen, dauert es mehrere hundert Tage, um den Cache zu füllen.

Die einfachste Methode zur Ermittlung der benötigten Cache-Größe geht von der maximalen Übertragungsrate der Verbindung aus. Bei einer Verbindung mit 1 Mbit/s beträgt die maximale Übertragungsrate 125 KB/s. Wenn dieser Datenverkehr vollständig im Cache gespeichert wird, ergeben sich in einer Stunde 450 MB. Dadurch würden bei 8 Arbeitsstunden 3,6 GB an einem einzigen Tag erreicht. Da normalerweise nicht das gesamte Volumen der Verbindung ausgeschöpft wird, kann angenommen werden, dass das Gesamtdatenvolumen, das auf den Cache zukommt, bei etwa 2 GB liegt. Daher sind bei diesem Beispiel 2 GB Festplattenspeicher erforderlich, damit Squid die durchsuchten Daten eines Tags im Cache speichern kann.

29.2.3 RAM

Der von Squid benötigte Arbeitsspeicher (RAM) steht in direktem Verhältnis zur Anzahl der Objekte im Cache. Außerdem speichert Squid Cache-Objekt-Bezüge und häufig angeforderte Objekte im Hauptspeicher, um das Abrufen dieser Daten zu beschleunigen. RAM ist wesentlich schneller als eine Festplatte.

Außerdem gibt es andere Daten, die Squid im Arbeitsspeicher benötigt, beispielsweise eine Tabelle mit allen IP-Adressen, einen exakten Domänennamen-Cache, die am häufigsten angeforderten Objekte, Zugriffssteuerungslisten, Puffer usw.

Es ist sehr wichtig, dass genügend Arbeitsspeicher für den Squid-Vorgang zur Verfügung steht, da die Systemleistung erheblich eingeschränkt ist, wenn ein Wechsel auf die Festplatte erforderlich ist. Das Werkzeug cachemgr.cgi kan für die Arbeitsspeicherverwaltung des Cache verwendet werden. Dieses Werkzeug wird in Abschnitt 29.6, „cachemgr.cgi“ (S. 488) behandelt. Bei Sites mit extrem hohem Netzwerkverkehr sollte ein AMD64- oder intel64;-System mit mehr als 4 GB Arbeitsspeicher verwendet werden.

29.2.4 Prozessor

Die Verwendung von Squid bringt keine intensive CPU-Auslastung mit sich. Die Prozessorlast wird nur erhöht, während die Inhalte des Cache geladen oder überprüft werden. Durch die Verwendung eines Computers mit mehreren Prozessoren wird die System-

leistung nicht erhöht. Um die Effizienz zu steigern, sollten vielmehr schnellere Festplatten oder ein größerer Arbeitsspeicher verwendet werden.

29.3 Starten von Squid

Squid ist in SUSE® Linux Enterprise Server bereits vorkonfiguriert. Sie können das Programm unmittelbar nach der Installation starten. Um einen reibungslosen Start zu gewährleisten, sollte das Netzwerk so konfiguriert werden, dass mindestens ein Namenserver und das Internet erreicht werden können. Es können Probleme auftreten, wenn eine Einwahlverbindung zusammen mit einer dynamischen DNS-Konfiguration verwendet wird. In diesem Fall sollte zumindest der Namenserver eingegeben werden, da Squid nicht startet, wenn kein DNS-Server in `/etc/resolv.conf` gefunden wird.

29.3.1 Befehle zum Starten und Stoppen von Squid

Geben Sie zum Starten von Squid als `root` in der Kommandozeile den Befehl `rcsquid start` ein. Beim ersten Start muss zunächst die Verzeichnisstruktur des Cache in `/var/cache/squid` definiert werden. Dies geschieht automatisch über das Startskript `/etc/init.d/squid` und kann einige Sekunden oder sogar Minuten in Anspruch nehmen. Wenn rechts in grüner Schrift `done` angezeigt wird, wurde Squid erfolgreich geladen. Um die Funktionsfähigkeit von Squid im lokalen System zu testen, geben Sie `localhost` als Proxy und `3128` als Port im Browser an.

Um Benutzern aus dem lokalen System und anderen Systemen den Zugriff auf Squid und das Internet zu ermöglichen, müssen Sie den Eintrag in den Konfigurationsdateien `/etc/squid/squid.conf` von `http_access deny all` in `http_access allow all` ändern. Beachten Sie dabei jedoch, dass dadurch jedem der vollständige Zugriff auf Squid ermöglicht wird. Daher sollten Sie ACLs definieren, die den Zugriff auf den Proxy steuern. Weitere Informationen hierzu finden Sie in Abschnitt 29.4.2, „Optionen für die Zugriffssteuerung“ (S. 482).

Nach der Bearbeitung der Konfigurationsdatei `/etc/squid/squid.conf` muss Squid die Konfigurationsdatei erneut laden. Verwenden Sie hierfür `rcsquidreload`.

Alternativ können Sie mit `rcsquid restart` einen vollständigen Neustart von Squid durchführen.

Mit dem Befehl `rcsquidstatus` können Sie überprüfen, ob der Proxy ausgeführt wird. Mit dem Befehl `rcsquidstop` wird Squid heruntergefahren. Dieser Vorgang kann einige Zeit in Anspruch nehmen, da Squid bis zu einer halben Minute (Option `shutdown_lifetime` in `/etc/squid/squid.conf`) wartet, bevor es die Verbindungen zu den Clients trennt und seine Daten auf die Festplatte schreibt.

WARNUNG: Beenden von Squid

Das Beenden von Squid mit `kill` oder `killall` kann den Cache beschädigen. Damit Squid neu gestartet werden kann, muss der beschädigte Cache gelöscht werden.

Wenn Squid nach kurzer Zeit nicht mehr funktioniert, obwohl das Programm erfolgreich gestartet wurde, überprüfen Sie, ob ein fehlerhafter Namenservereintrag vorliegt oder ob die Datei `/etc/resolv.conf` fehlt. Squid protokolliert die Ursache eines Startfehlers in der Datei `/var/log/squid/cache.log`. Wenn Squid beim Booten des Systems automatisch geladen werden soll, müssen Sie Squid mithilfe des YaST-Runlevel-Editors für die gewünschten Runlevels aktivieren. Weitere Informationen hierzu finden Sie unter Abschnitt 7.2.3, „Konfigurieren von Systemdiensten (Runlevel) mit YaST“ (S. 78).

Durch eine Deinstallation von Squid werden weder die Cache-Hierarchie noch die Protokolldateien entfernt. Um diese zu entfernen, müssen Sie das Verzeichnis `/var/cache/squid` manuell löschen.

29.3.2 Lokaler DNS-Server

Die Einrichtung eines lokalen DNS-Servers ist sinnvoll, selbst wenn er nicht seine eigene Domäne verwaltet. Er fungiert dann einfach als Nur-Cache-Namenserver und kann außerdem DNS-Anforderungen über die Root-Namenserver auflösen, ohne dass irgendeine spezielle Konfiguration erforderlich ist (siehe Abschnitt 21.4, „Starten des Namenservers BIND“ (S. 326)). Wie dies durchgeführt werden kann, hängt davon ab, ob Sie bei der Konfiguration der Internetverbindung dynamisches DNS auswählen.

Dynamisches DNS

Normalerweise wird bei dynamischem DNS der DNS-Server während des Aufbaus der Internetverbindung vom Anbieter festgelegt und die lokale Datei `/etc/resolv.conf` wird automatisch angepasst. Dieses Verhalten wird in der Datei `/etc/sysconfig/network/config` mit der sysconfig-Variablen `MODIFY_RESOLV_CONF_DYNAMICALLY` gesteuert, die auf `"yes"` eingestellt ist. Stellen Sie diese Variable mit dem sysconfig-Editor von YaST auf `"no"` ein (siehe Abschnitt 7.3.1, „Ändern der Systemkonfiguration mithilfe des YaST-Editors "sysconfig"“ (S. 80)). Geben Sie anschließend den lokalen DNS-Server in die Datei `/etc/resolv.conf` ein. Verwenden Sie die IP-Adresse `127.0.0.1` für `localhost`. Auf diese Weise kann Squid immer den lokalen Namenserver finden, wenn er gestartet wird.

Um den Zugriff auf den Namenserver des Anbieters zu ermöglichen, geben Sie ihn zusammen mit seiner IP-Adresse in die Konfigurationsdatei `/etc/named.conf` unter `forwarders` ein. Mit dynamischem DNS kann dies automatisch während des Verbindungsaufbaus erreicht werden, indem die sysconfig-Variable `MODIFY_NAMED_CONF_DYNAMICALLY` auf `YES` gesetzt wird.

Statisches DNS

Beim statischen DNS finden beim Verbindunsgsaufbau keine automatischen DNS-Anpassungen statt, sodass auch keine sysconfig-Variablen geändert werden müssen. Sie müssen jedoch den lokalen DNS-Server in die Datei `/etc/resolv.conf` eingeben, wie oben beschrieben. Außerdem muss der statische Namenserver des Anbieters zusammen mit seiner IP-Adresse manuell in die Datei `/etc/named.conf` unter `forwarders` eingegeben werden.

TIPP: DNS und Firewall

Wenn eine Firewall ausgeführt wird, müssen Sie sicherstellen, dass DNS-Anforderungen durchgelassen werden.

29.4 Die Konfigurationsdatei /etc/squid/squid.conf

Alle Einstellungen für den Squid-Proxyserver werden in der Datei `/etc/squid/squid.conf` vorgenommen. Beim ersten Start von Squid sind keine Änderungen in dieser Datei erforderlich, externen Clients wird jedoch ursprünglich der Zugriff verweigert. Der Proxy ist für `localhost` verfügbar. Der Standardport ist `3128`. Die vorinstallierte Konfigurationsdatei `/etc/squid/squid.conf` bietet detaillierte Informationen zu den Optionen sowie zahlreiche Beispiele. Fast alle Einträge beginnen mit # (kommentierte Zeilen) und die relevanten Spezifikationen befinden sich am Ende der Zeile. Die angegebenen Werte korrelieren fast immer mit den Standardwerten, sodass das Entfernen der Kommentarzeichen ohne Ändern der Parameter in den meisten Fällen kaum Auswirkungen hat. Lassen Sie die Beispiele nach Möglichkeit unverändert und geben Sie die Optionen zusammen mit den geänderten Parametern in der Zeile darunter ein. Auf diese Weise können die Standardwerte problemlos wiederhergestellt und mit den Änderungen verglichen werden.

TIPP: Anpassen der Konfigurationsdatei nach einer Aktualisierung

Wenn Sie eine Aktualisierung einer früheren Squid-Version durchgeführt haben, sollten Sie die neue Datei `/etc/squid/squid.conf` bearbeiten und nur die in der vorherigen Datei vorgenommenen Änderungen übernehmen. Wenn Sie versuchen, die alte `squid.conf` zu verwenden, besteht das Risiko, dass die Konfiguration nicht mehr funktioniert, da die Optionen manchmal bearbeitet und neue Änderungen hinzugefügt werden.

29.4.1 Allgemeine Konfigurationsoptionen (Auswahl)

http_port 3128

Dies ist der Port, den Squid auf Client-Anforderungen überwacht. Der Standardport ist `3128`, `8080` wird jedoch ebenfalls häufig verwendet. Sie können auch mehrere Portnummern durch Leerzeichen getrennt eingeben.

cache_peer *hostnametypeproxy-porticp-port*

Geben Sie hier einen übergeordneten Proxy ein, beispielsweise wenn Sie den Proxy Ihres ISP verwenden möchten. Geben Sie als *hostname* den Namen oder die IP-Adresse des zu verwendenden Proxy und als *type* `parent` ein. Geben Sie als *proxy-port* die Portnummer ein, die ebenfalls vom Operator des Parent für die Verwendung im Browser angegeben wurde, in der Regel `8080`. Setzen Sie *icp-port* auf `7` oder `0`, wenn der ICP-Port des übergeordneten Proxy nicht bekannt ist und seine Verwendung für den Anbieter nicht wichtig ist. Außerdem können `default` und `no-query` nach den Portnummern angegeben werden, um die Verwendung des ICP-Protokolls zu verhindern. Squid verhält sich dann in Bezug auf den Proxy des Anbieters wie ein normaler Browser.

cache_mem 8 MB

Dieser Eintrag legt fest, wie viel Arbeitsspeicher Squid für besonders beliebte Antworten verwenden kann. Der Standardwert ist `8 MB`. Dieser Wert gibt nicht die Arbeitsspeichernutzung von Squid an und kann überschritten werden.

cache_dir ufs /var/cache/squid/ 100 16 256

Der Eintrag *cache_dir* legt das Verzeichnis fest, in dem alle Objekte auf dem Datenträger gespeichert werden. Die Zahlen am Ende geben den maximal zu verwendenden Festplattenspeicher in BM und die Anzahl der Verzeichnisse auf der ersten und zweiten Ebene an. Der Parameter `ufs` sollte nicht geändert werden. Standardmäßig werden 100 MB Speicherplatz im Verzeichnis `/var/cache/squid` belegt und 16 Unterverzeichnisse erstellt, die wiederum jeweils 256 Unterverzeichnisse aufweisen. Achten Sie bei der Angabe des zu verwendenden Speicherplatzes darauf, genügend Reserve einzuplanen. Werte von mindestens 50 bis maximal 80 % des verfügbaren Speicherplatzes erscheinen hier am sinnvollsten. Die letzten beiden Werte für die Verzeichnisse sollten nur nach reiflicher Überlegung erhöht werden, da zu viele Verzeichnisse ebenfalls zu Leistungsproblemen führen können. Wenn der Cache von mehreren Datenträgern gemeinsam verwendet wird, müssen Sie mehrere *cache_dir*-Zeilen eingeben.

cache_access_log /var/log/squid/access.log , cache_log /var/log/squid/cache.log , cache_store_log /var/log/squid/store.log

Diese drei Einträge geben an, in welchen Pfad Squid alle Aktionen protokolliert. Normalerweise werden hier keine Änderungen vorgenommen. Bei hoher Auslastung von Squid kann es sinnvoll sein, Cache und Protokolldateien auf mehrere Datenträger zu verteilen.

emulate_httpd_log off
: Wenn der Eintrag auf *on* gesetzt ist, erhalten Sie lesbare Protokolldateien. Einige Evaluierungsprogramme können solche Dateien jedoch nicht interpretieren.

client_netmask 255.255.255.255
: Mit diesem Eintrag werden die IP-Adressen von Clients in den Protokolldateien maskiert. Die letzte Ziffer der IP-Adresse wird auf 0 gesetzt, wenn Sie hier `255.255.255.0` eingeben. Auf diese Weise können Sie den Datenschutz für die Clients gewährleisten.

ftp_user Squid@
: Mit dieser Option wird das Passwort festgelegt, das Squid für die anonyme FTP-Anmeldung verwenden soll. Es kann sinnvoll sein, hier eine gültige E-Mail-Adresse anzugeben, da einige FTP-Server die Adressen auf Gültigkeit prüfen.

cache_mgr webmaster
: Eine E-Mail-Adresse, an die Squid eine Meldung sendet, wenn es plötzlich abstürzt. Der Standardwert ist *webmaster*.

logfile_rotate 0
: Wenn Sie `squid -k rotate` ausführen, kann `Squid` ein Rotationssystem für gesicherte Protokolldateien einführen. Bei diesem Prozess werden die Dateien nummeriert und nach dem Erreichen des angegebenen Werts wird die älteste Datei überschrieben. Der Standardwert ist `0`, da das Archivieren und Löschen von Protokolldateien in SUSE Linux Enterprise Server von einem in der Konfigurationsdatei `/etc/logrotate/squid` festgelegten Cronjob durchgeführt wird.

append_domain <Domaene>
: Mit *append_domain* können Sie angeben, welche Domäne automatisch angefügt wird, wenn keine angegeben wurde. Normalerweise wird hier die eigene Domäne angegeben, sodass bei der Eingabe von *www* im Browser ein Zugriff auf Ihren eigenen Webserver erfolgt.

forwarded_for on
: Wenn Sie den Eintrag auf *off* setzen, entfernt Squid die IP-Adresse und den Systemnamen des Client aus den HTTP-Anforderungen. Anderenfalls wird eine Zeile zum Header hinzugefügt, beispielsweise:

```
X-Forwarded-For: 192.168.0.1
```

negative_ttl 5 minutes; negative_dns_ttl 5 minutes

Die hier angegebenen Werte müssen in der Regel nicht geändert werden. Bei einer Einwahlverbindung kann das Internet jedoch zeitweise nicht verfügbar sein. Squid protokolliert die nicht erfolgreichen Anforderungen und lässt dann keine weiteren zu, auch wenn die Internetverbindung zwischenzeitlich wieder hergestellt wurde. In solchen Fällen sollten Sie *minutes* in *seconds* ändern. Danach sollte nach dem Klicken auf *Neu laden* im Browser der Einwahlvorgang nach wenigen Sekunden wieder aktiviert werden.

never_direct allow *ACL-Name*

Um zu verhindern, dass Squid Anforderungen direkt aus dem Internet entgegennimmt, müssen Sie mit dem oben stehenden Befehl die Verbindung mit einem anderen Proxy erzwingen. Dieser muss zuvor unter *cache_peer* eingegeben worden sein. Wenn als *acl_name* `all` angegeben wird, werden alle Anforderungen zwangsweise direkt an den übergeordneten Proxy (*parent*) weitergeleitet. Dies kann beispielsweise dann erforderlich sein, wenn Sie einen Anbieter verwenden, der die Verwendung der eigenen Proxies strikt vorschreibt oder der durch seine Firewall direkten Internetzugriff verweigert.

29.4.2 Optionen für die Zugriffssteuerung

Squid bietet ein detailliertes System für die Steuerung des Zugriffs auf den Proxy. Durch die Implementierung von ACLs kann es problemlos und umfassend konfiguriert werden. Dazu gehören Listen mit Regeln, die nacheinander verarbeitet werden. Die ACLs müssen zuerst definiert werden, bevor sie verwendet werden können. Einige Standard-ACLs, wie beispielsweise *all* und *localhost*, sind bereits vorhanden. Die bloße Definition einer ACL bedeutet jedoch noch nicht, dass sie tatsächlich angewendet wird. Dies geschieht nur in Verbindung mit *http_access*-Regeln.

acl <ACL-Name> <Typ> <Daten>

Für die Definition eines ACL sind mindestens drei Spezifikationen erforderlich. Der Name <*ACL-Name*> kann frei gewählt werden. Als <*Typ*> können Sie aus einer Vielzahl verschiedener Optionen wählen, die Sie im Abschnitt *ACCESS CONTROLS* in der Datei `/etc/squid/squid.conf` finden. Die Spezifikation für <*Daten*> hängt vom einzelnen ACL-Typ ab und kann auch aus einer Datei gelesen werden, beispielsweise über Hostnamen, IP-Adressen oder URLs. Im Folgenden finden Sie einige einfache Beispiele:

```
acl mysurfers srcdomain .my-domain.com
```

```
acl teachers src 192.168.1.0/255.255.255.0
acl students src 192.168.7.0-192.168.9.0/255.255.255.0
acl lunch time MTWHF 12:00-15:00
```

http_access allow <ACL-Name>

http_access legt fest, wer den Proxy verwenden kann und wer auf welche Seiten im Internet zugreifen kann. Hierfür müssen ACLs angegeben werden. *localhost* und *all* wurden bereits oben definiert. Diese Optionen können den Zugriff über *deny* oder *allow* verweigern oder zulassen. Es können Listen mit einer beliebigen Anzahl von *http_access*- Einträgen erstellt und von oben nach unten verarbeitet werden. Je nachdem, was zuerst vorkommt, wird der Zugriff auf die betreffende URL gestattet oder verweigert. Der letzte Eintrag muss immer *http_access deny all* sein. Im folgenden Beispiel hat *localhost* freien Zugriff auf alle Elemente, während allen anderen Hosts der Zugriff vollständig verweigert wird.

```
http_access allow localhost
http_access deny all
```

In einem anderen Beispiel, bei dem diese Regeln verwendet werden, hat die Gruppe `teachers` immer Zugriff auf das Internet. Die Gruppe `students` erhält nur montags bis freitags während der Mittagspause Zugriff.

```
http_access deny localhost
http_access allow teachers
http_access allow students lunch time
http_access deny all
```

Die Liste mit den *http_access*-Einträgen sollte um der besseren Lesbarkeit willen nur an der angegebenen Position in der Datei `/etc/squid/squid.conf` eingegeben werden. Also zwischen dem Text

```
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR
# CLIENTS
```

und dem letzten

```
http_access deny all
```

redirect_program /usr/bin/squidGuard

Mit dieser Option können Sie eine Umleitungsfunktion, wie beispielsweise squidGuard, angeben, die das Blockieren unerwünschter URLs ermöglicht. Der Internetzugang kann mithilfe der Proxy-Authentifizierung und der entsprechenden ACLs

individuell für verschiedene Benutzergruppen gesteuert werden. squidGuard ist ein gesondertes Paket, das installiert und konfiguriert werden kann.

auth_param basic program /usr/sbin/pam_auth
: Wenn die Benutzer auf dem Proxy authentifiziert werden müssen, geben Sie ein entsprechendes Programm an, beispielsweise pam_auth. Beim ersten Zugriff auf pam_auth wird dem Benutzer ein Anmeldefenster angezeigt, in das er den Benutzernamen und das Passwort eingeben muss. Außerdem ist noch immer eine ACL erforderlich, sodass nur Clients mit einer gültigen Anmeldung das Internet benutzen können.

```
acl password proxy_auth REQUIRED

http_access allow password
http_access deny all
```

: Das *REQUIRED* nach *proxy_auth* kann durch eine Liste der zulässigen Benutzernamen oder durch den Pfad zu einer solchen Liste ersetzt werden.

ident_lookup_access allow <ACL-Name>
: Lassen Sie damit eine ident-Anforderung für alle ACL-definierten Clients ausführen, um die Identität der einzelnen Benutzer zu ermitteln. Wenn Sie *all* auf *<ACL-Name>* anwenden, gilt dies für alle Clients. Außerdem muss ein ident-Daemon auf allen Clients ausgeführt werden. Bei Linux installieren Sie zu diesem Zweck das Paket "pidentd". Für Microsoft Windows steht kostenlose Software zum Herunterladen aus dem Internet zur Verfügung. Um sicherzustellen, dass nur Clients mit einem erfolgreichen ident-Lookup zulässig sind, definieren Sie hier eine entsprechende ACL:

```
acl identhosts ident REQUIRED

http_access allow identhosts
http_access deny all
```

: Ersetzen Sie auch hier *REQUIRED* durch eine Liste der zulässigen Benutzernamen. Durch die Verwendung von *ident* kann die Zugriffszeit erheblich reduziert werden, da die ident-Lookups für jede Anforderung wiederholt werden.

29.5 Konfigurieren eines transparenten Proxy

In der Regel arbeiten Sie folgendermaßen mit Proxyservern: der Web-Browser sendet Anforderungen an einen bestimmten Port im Proxyserver und der Proxy liefert die angeforderten Objekte unabhängig davon, ob sie sich im Cache befinden oder nicht. Bei der Arbeit in einem Netzwerk können verschiedene Situationen entstehen:

- Aus Sicherheitsgründen sollten alle Clients einen Proxy für den Zugriff auf das Internet verwenden.
- Alle Clients müssen einen Proxy verwenden, unabhängig davon, ob sie sich dessen bewusst sind.
- Der Proxy in einem Netzwerk wird verschoben, die vorhandenen Clients sollten jedoch ihre alte Konfiguration beibehalten.

In all diesen Fällen kann ein transparenter Proxy verwendet werden. Das Prinzip ist einfach: Der Proxy fängt die Anforderungen des Webbrowsers ab und beantwortet sie. Der Webbrowser erhält die angeforderten Seiten, ohne zu wissen, woher sie kommen. Wie der Name schon andeutet, verläuft der gesamte Prozess transparent.

29.5.1 Konfigurationsoptionen in /etc/squid/squid.conf

Um squid mitzuteilen, dass es als ein transparenter Proxy fungieren soll, verwenden Sie die Option `transparent` am Tag `http_port` in der Hauptkonfigurationsdatei `/etc/squid/squid.conf`. Nach dem Neustart von squid muss nur noch die Firewall neu umkonfiguriert werden, damit sie den HTTP-Port an den Port umleitet, der in `http_port` angegeben ist. In der folgenden squid-Konfigurationszeile wäre dies der Port 3128.

```
http_port 3128 transparent
```

29.5.2 Firewall-Konfiguration mit SuSEfirewall2

Leiten Sie nun alle eingehenden Anforderungen über die Firewall mithilfe einer Port-Weiterleitungsregel an den Squid-Port um. Verwenden Sie dazu das eingeschlossene Werkzeug SuSEfirewall2 (in Abschnitt „Configuring the Firewall with YaST“ (Kapitel 8, *Masquerading and Firewalls*, ↑*Security Guide*) beschrieben). Die Konfigurationsdatei dieses Programms finden Sie in `/etc/sysconfig/SuSEfirewall2`. Die Konfigurationsdatei besteht aus gut dokumentierten Einträgen. Um einen transparenten Proxy festzulegen, müssen Sie mehrere Firewall-Optionen konfigurieren:

- Gerät zeigt auf das Internet: `FW_DEV_EXT`="eth1"
- Gerät zeigt auf das Netzwerk: `FW_DEV_INT`="eth0"

Definieren Sie Ports und Dienste (siehe `/etc/services`) auf der Firewall, auf die ein Zugriff von nicht verbürgten (externen) Netzwerken, wie beispielsweise dem Internet, erfolgt. In diesem Beispiel werden nur Webdienste für den Außenbereich angeboten:

```
FW_SERVICES_EXT_TCP="www"
```

Definieren Sie Ports und Dienste (siehe `/etc/services`) auf der Firewall, auf die vom sicheren (internen) Netzwerk aus zugegriffen wird (sowohl über TCP als auch über UDP):

```
FW_SERVICES_INT_TCP="domain www 3128"
FW_SERVICES_INT_UDP="domain"
```

Dies ermöglicht den Zugriff auf Webdienste und Squid (Standardport: `3128`). Der Dienst "domain" steht für DNS (Domain Name Service, Domänennamen-Dienst). Dieser Dienst wird häufig verwendet. Andernfalls nehmen Sie einfach die oben stehenden Einträge heraus und setzten Sie die folgende Option auf `no`:

```
FW_SERVICE_DNS="yes"
```

Die wichtigste Option ist Option Nummer `15`:

Beispiel 29.1 *Firewall-Konfiguration: Option 15*

```
# 15.)
# Which accesses to services should be redirected to a local port on
# the firewall machine?
#
# This option can be used to force all internal users to surf via
# your squid proxy, or transparently redirect incoming webtraffic to
# a secure webserver.
#
# Format:
# list of <source network>[,<destination network>,<protocol>[,dport[:lport]]
# Where protocol is either tcp or udp. dport is the original
# destination port and lport the port on the local machine to
# redirect the traffic to
#
# An exclamation mark in front of source or destination network
# means everything EXCEPT the specified network
#
# Example: "10.0.0.0/8,0/0,tcp,80,3128 0/0,172.20.1.1,tcp,80,8080"
```

Die oben angegebenen Kommentare geben die zu verwendende Syntax an. Geben Sie zuerst die IP-Adresse und die Netzmaske der internen Netzwerke ein, die auf die Proxy-Firewall zugreifen. Geben Sie als Zweites die IP-Adresse und die Netzmaske ein, an die diese Clients ihre Anforderungen senden. Geben Sie bei Webbrowsern die Netzwerke `0/0` an. Dieser Platzhalter bedeutet "überallhin"."" Geben Sie anschließend den ursprünglichen Port ein, an den diese Anforderungen gesendet werden, und schließlich den Port, an den alle diese Anforderungen umgeleitet werden. Da Squid andere Protokolle als HTTP unterstützt, müssen Anforderungen von anderen Ports an den Proxy umgeleitet werden, beispielsweise FTP (Port 21), HTTPS oder SSL (Port 443). In diesem Beispiel werden Webdienste (Port `80`) an den Proxy-Port (Port `3128`) umgeleitet. Wenn mehrere Netzwerke bzw. Dienste hinzugefügt werden sollen, müssen diese im entsprechenden Eintrag durch ein Leerzeichen getrennt sein.

```
FW_REDIRECT="192.168.0.0/16,0/0,tcp,80,3128"
```

Um die Firewall mit der neuen Konfiguration zu starten, müssen Sie einen Eintrag in der Datei `/etc/sysconfig/SuSEfirewall2` ändern. Der Eintrag `START_FW` muss auf `"yes"` gesetzt werden.

Starten Sie Squid wie in Abschnitt 29.3, „Starten von Squid“ (S. 476) gezeigt. Um zu überprüfen, ob alles ordnungsgemäß funktioniert, müssen Sie die Squid-Protokolle in `/var/log/squid/access.log` überprüfen. Um sicherzustellen, dass alle Ports korrekt konfiguriert sind, führen Sie auf dem Rechner von einem beliebigen Rechner außerhalb des Netzwerks eine Portscan durch. Nur die Webdienste (Port 80) sollten

verfügbar sein. Die Befehlssyntax für das Scannen der Ports mit nmap lautet `nmap -O IP_address`.

29.6 cachemgr.cgi

Der Cache-Manager (cachemgr.cgi) ist ein CGI-Dienstprogramm für die Anzeige der Statistiken zur Arbeitsspeichernutzung eines laufenden Squid-Prozesses. Außerdem bietet er eine bequemere Methode zur Verwaltung des Cache und zur Anzeige der Statistiken ohne Anmeldung beim Server.

29.6.1 Einrichtung

Zunächst muss ein Webserver in Ihrem System ausgeführt werden. Konfigurieren Sie Apache, wie in Kapitel 27, *Der HTTP-Server Apache* (S. 419) beschrieben. Um zu überprüfen, ob Apache bereits ausgeführt wird, geben Sie als `root` den Befehl `rcapachestatus ein`. Wenn eine Meldung der folgenden Art angezeigt wird:

```
Checking for service httpd: OK
Server uptime: 1 day 18 hours 29 minutes 39 seconds
```

wird Apache auf dem Rechner angezeigt. Geben Sie andernfalls `rcapachestart` ein, um Apache mit den Standardeinstellungen von SUSE Linux Enterprise Server zu starten. Der letzte Schritt besteht darin, die Datei `cachemgr.cgi` in das Apache-Verzeichnis `cgi-bin` zu kopieren. Für 32-Bit funktioniert das wie folgt:

```
cp /usr/lib/squid/cachemgr.cgi /srv/www/cgi-bin/
```

In einer 64-Bit-Umgebung befindet sich die Datei `cachemgr.cgi` unter `/usr/lib64/squid/` und das Kommando, sie in das Apache-Verzeichnis zu kopieren, lautet:

```
cp /usr/lib64/squid/cachemgr.cgi /srv/www/cgi-bin/
```

29.6.2 Cache-Manager-ACLs in /etc/squid/squid.conf

Es gibt einige Standardeinstellungen in der Originaldatei, die für den Cache-Manager erforderlich sind. Zuerst werden zwei ACLs definiert. Anschließend verwenden die http_access-Optionen diese ACLs, um Zugriff vom CGI-Script auf Squid zu gewähren. Die erste ACL ist die wichtigste, da der Cache-Manager versucht, über das cache_object-Protokoll mit Squid zu kommunizieren.

```
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
```

Folgende Regeln gewähren Apache Zugriffsrechte auf Squid:

```
http_access allow manager localhost
http_access deny manager
```

Diese Regeln setzen voraus, dass der Webserver und Squid auf demselben Computer ausgeführt werden. Wenn die Kommunikation zwischen Cache-Manager und Squid von dem Webserver auf einem anderen Computer ihren Ausgang nimmt, müssen Sie eine zusätzliche ACL aufnehmen, wie in Beispiel 29.2, „Zugriffsregeln“ (S. 489) beschrieben.

Beispiel 29.2 *Zugriffsregeln*

```
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl webserver src 192.168.1.7/255.255.255.255 # webserver IP
```

Fügen Sie dann die Regeln in Beispiel 29.3, „Zugriffsregeln“ (S. 489) hinzu, um den Zugriff vom Webserver zu gestatten.

Beispiel 29.3 *Zugriffsregeln*

```
http_access allow manager localhost
http_access allow manager webserver
http_access deny manager
```

Konfigurieren Sie ein Passwort für den Manager für den Zugriff auf weitere Optionen, wie das Schließen des Cache über entfernten Zugriff oder die Anzeige weiterer Informationen zum Cache. Konfigurieren Sie hierfür den Eintrag `cachemgr_passwd` mit

einem Passwort für den Manager und der Liste der anzuzeigenden Optionen. Diese Liste wird als Teil des Eintragskommentars in `/etc/squid/squid.conf` angezeigt.

Starten Sie Squid nach jeder Änderung der Konfigurationsdatei neu. Verwenden Sie hierfür einfach `rcsquidreload`.

29.6.3 Anzeige der Statistiken

Rufen Sie die entsprechende Website auf: `http://webserver.example.org/cgi-bin/cachemgr.cgi`. Drücken Sie *continue* (Fortsetzen) und blättern Sie durch die verschiedenen Statistiken. Weitere Details für die einzelnen, vom Cache-Manager angezeigten Einträge finden Sie in den Squid FAQ unter `http://www.squid-cache.org/Doc/FAQ/FAQ-9.html`.

29.7 Erstellung von Cache-Berichten mit Calamaris

Calamaris ist ein Perl-Skript, mit dem Berichte über die Cache-Aktivität im ASCII- oder HTML-Format erstellt werden können. Es arbeitet mit nativen Squid-Zugriffsprotokolldateien. Die Calamaris-Homepage befindet sich unter `http://Calamaris.Cord.de/`. Das Programm ist recht benutzerfreundlich.

Melden Sie sich als `root` an und geben Sie `cat access.log | calamaris` *`options`* `> reportfile` ein. Beim Piping mehrerer Protokolldateien ist darauf zu achten, dass die Protokolldateien chronologisch (die ältesten Dateien zuerst) geordnet sind. Im Folgenden finden Sie einige Optionen des Programms:

TIPP: Shell und Dateisequenzen

Wenn Sie über mehrere ähnliche Dateien verfügen, z. B. `access.log.1`, `access.log.2` usw., würde die Standard-Bash-Shell diese Dateien beim Auflisten von `access.log nicht in der Zahlensequenz sortieren.*`. Um dieses Problem zu lösen, können Sie die Syntax `access.log{1..42}` verwenden, die eine Liste von Dateien, erweitert durch Nummern von 1 bis 42, generiert.

-a
: Ausgabe aller verfügbaren Berichte

-w
: Ausgabe als HTML-Bericht

-l
: Einschließen einer Meldung oder eines Logos in den Berichtsheader

Weitere Informationen zu den verschiedenen Optionen finden Sie auf der man-Seite des Programms `mancalamaris`.

Typisches Beispiel:

```
cat access.log.{10..1} access.log | calamaris -a -w \
> /usr/local/httpd/htdocs/Squid/squidreport.html
```

Dadurch wird der Bericht im Verzeichnis des Webservers gespeichert. Zur Anzeige des Berichts ist Apache erforderlich.

29.8 Weiterführende Informationen

Besuchen Sie die Squid-Homepage unter `http://www.squid-cache.org/`. Hier finden Sie das Squid-Benutzerhandbuch und eine umfassende Sammlung mit FAQ zu Squid.""

Nach der Installation ist eine kleine HOWTO-Datei zu transparenten Proxies in `howtoenh` verfügbar: `/usr/share/doc/howto/en/txt/TransparentProxy.gz`. Außerdem sind Mailinglisten für Squid unter `squid-users@squid-cache.org` verfügbar. Das zugehörige Archiv finden Sie unter `http://www.squid-cache.org/mail-archive/squid-users/`.